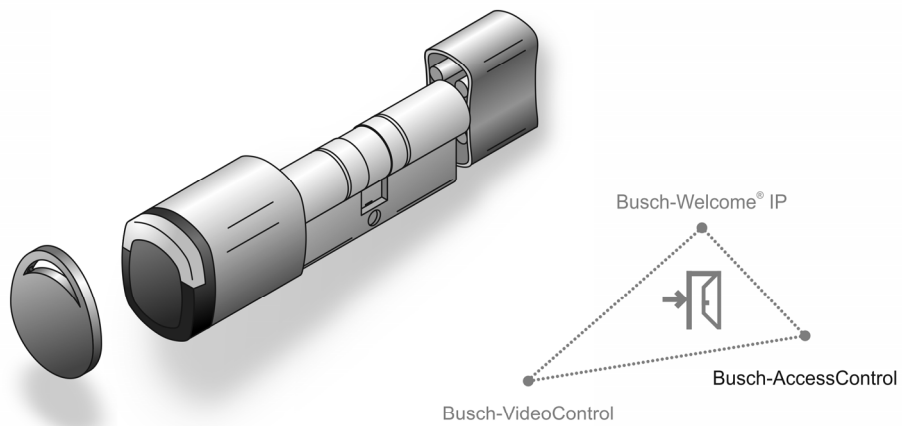


Busch-AccessControl



1	Übersicht.....	5
1.1	Hinweise zum Handbuch	5
1.2	Zielgruppe / Qualifikation des Personals	6
1.3	Einführung in Busch-AccessControl	6
1.4	Busch-AccessControl und smartIP	8
1.5	Grundlagen strukturierter Verkabelung	9
1.6	Designlinien.....	13
1.7	Grundlagen.....	13
2	Sortimentsübersicht.....	14
2.1	Einsatz.....	14
2.2	Anwendungsbereiche	15
2.3	Geräteübersicht.....	16
2.3.1	Aufbau der Artikelnummern.....	16
2.3.2	Schließzylinder	17
2.3.3	Systemgeräte	18
2.3.4	Zubehör.....	20
2.4	Montagemöglichkeiten	21
2.4.1	Voraussetzungen	21
2.4.2	Schließzylinder ausmessen.....	23
2.4.3	Alte Schließzylinder demontieren	25
3	Inbetriebnahme	28
3.1	Übersicht der Inbetriebnahme	28
3.2	Voraussetzungen	28
3.1	Inbetriebnahme des Systems — „Smart Access Point Pro“	30
3.1.1	Übersicht.....	30
3.1.2	Einen PC mit dem „Smart Access Point“ Verbinden	30
3.1.3	Vorabinformation: Auswahl der Systemmodi.....	32
3.1.4	„Smart Access Point“ in Betrieb nehmen.....	34
3.1.5	Vorabinformation: IP-Adresse an einem PC angleichen.....	41
3.2	Geräte hinzufügen.....	43
3.2.1	„Elektronischer Schließzylinder“	43
3.2.2	„Elektronischer Schließzylinder“ vorab hinzufügen.....	47
3.2.3	„RF/IP Gateway“	47
3.2.4	Repeater	48
3.3	Gerät löschen im „Smart Access Point“	50
3.3.1	„Elektronischer Schließzylinder“	50
3.3.2	„RF/IP Gateway“	50
3.3.3	Repeater	50
3.4	Projekt sichern / Wiederherstellen (Backup / Restore)	51
3.5	RESET (System / Geräte zurücksetzen)	53
3.5.1	„Smart Access Point“	53
4	Planungs- / Anwendungsinformationen	54
4.1	Funktionsprinzipien / Arbeitsweisen	54

4.2	Kapazität / Reichweite	57
4.3	Anwendungsbeispiele	61
4.3.1	Einfamilienhaus	61
4.3.2	Mehrfamilienhaus mit einem Geschoss	63
4.3.3	Mehrfamilienhaus mit mehreren Geschossen	65
4.3.4	Mehrfamilienhaus mit einer Arztpraxis	67
4.3.5	Wohngebäude mit einem längeren Geschoss	71
4.3.6	Wohngebäude mit mehreren Geschossen	75
4.3.7	Perimeter	79
4.4	Störquellen	85
5	Verwaltungssoftware im „Smart Access Point Pro“	86
5.1	Übersicht	86
5.2	Gerätekonfiguration	87
5.2.1	„Smart Access Point Pro“ hinzufügen	88
5.2.2	„Elektronischer Schließzylinder“ hinzufügen	89
5.2.3	„RF/IP Gateway“ hinzufügen	91
5.2.4	„RF Repeater“ hinzufügen	93
5.3	Gebäudestruktur	95
5.3.1	Gebäude anlegen	96
5.3.2	Etagen anlegen	99
5.3.3	Räume anlegen	101
5.4	Zutrittskontrolle	103
5.4.1	„Smart Access Point Pro“ platzieren	104
5.4.2	„RF/IP Gateway“ platzieren	107
5.4.3	„Elektronischer Schließzylinder“ platzieren	110
5.4.4	Elektronischer Schließzylinder mit Smart Access Point koppeln	112
5.4.5	Repeater platzieren	115
5.4.6	Repeater koppeln	116
5.5	Benutzerverwaltung	118
5.5.1	Benutzer anlegen	119
5.5.3	Authentifizierung hinzufügen	120
5.5.4	Schließrecht erteilen	125
5.6	Daten aus dem Menü "Benutzerverwaltung" löschen	127
5.6.1	Schließrecht löschen	128
5.6.2	Authentifizierung löschen	130
5.6.3	Benutzer löschen	132
5.7	Daten aus dem Menü "Zutrittskontrolle" löschen	134
5.7.1	Elektronischer Schließzylinder von Smart Access Point Pro entkoppeln	135
5.7.2	Elektronischer Schließzylinder aus dem Raum entfernen	138
5.7.3	Smart Access Point Pro aus dem Raum entfernen	139
5.7.4	Repeater entkoppeln	140
5.7.5	Repeater aus dem Raum entfernen	142
5.8	Daten aus dem Menü "Gerätekonfiguration" löschen	143
5.8.1	Elektronischer Schließzylinder aus dem System löschen	144
5.8.2	Smart Access Point Pro aus dem System löschen	145
5.8.3	Repeater aus dem System löschen	146
5.9	Daten aus dem Menü "Gebäudestruktur" löschen	147
5.9.1	Räume löschen	148

5.9.2	Etagen löschen	149
5.9.3	Gebäude löschen	150
6	Notizen	151
7	Index	152

1 Übersicht

1.1 Hinweise zum Handbuch

Dieses Handbuch beschreibt das System Busch-AccessControl. Es unterstützt Sie bei der Auswahl und Planung des richtigen Aufbaus.

Es beinhaltet eine Übersicht der bisher zur Verfügung stehenden Komponenten und gibt Anregungen zur sinnvollen Kombination und Integration.

Für detaillierte technische Informationen zu den einzelnen Komponenten beachten Sie bitte auch die jeweiligen Produktdokumentationen.

Unter Kapitel 4.3 „Anwendungsbeispiele“ auf Seite 61 wird die Thematik dieses Dokumentes anhand von Beispielen erläutert. Die Informationen in den Kapiteln bauen dabei aufeinander auf. Wenn Sie sich mit dem Thema neu oder wieder vertraut machen möchten, lesen Sie sich entsprechend alle Unterkapitel zu diesem Thema durch.

1.2 Zielgruppe / Qualifikation des Personals

Die Installation, Inbetriebnahme und Wartung des Geräts darf nur durch dafür ausgebildete Elektrofachkräfte mit entsprechender Qualifikation erfolgen.

Die Elektrofachkraft muss das Handbuch gelesen und verstanden haben und den Anweisungen folgen.

Die Elektrofachkraft muss die in ihrem Land geltenden nationalen Vorschriften bezüglich Installation, Funktionsprüfung, Reparatur und Wartung von elektrischen Produkten beachten.

Die Fachkraft muss über allgemeine Netzwerk-Kenntnisse verfügen.

1.3 Einführung in Busch-AccessControl

Die „Elektronischer Schließzylinder“ sind für den Einsatz innerhalb des IP-Systems Busch-AccessControl konzipiert und vorgesehen.

Kommunikation und Strom

Die Kommunikation der „Elektronischer Schließzylinder“ erfolgt über Bluetooth. Eine separate Stromversorgung ist nicht notwendig. Die „Elektronischer Schließzylinder“ beziehen die notwendige Energie über mitgelieferte Batterien.

Skalierbarkeit

Kleinere Objekte lassen sich ebenso installieren, wie große Projekte. Bereits bestehende Installationen lassen sich zu jeder Zeit erweitern.

Bedienung

Zentrale Verwaltung aller Zutrittspunkte über die App Busch-Welcome® App.

Schlüsselverlust

Kein Hardwaretausch, wenn Schlüssel verloren gehen.

Neu oder Nachrüsten

Die „Elektronischer Schließzylinder“ lassen sich an nahezu allen Türen einbauen. Entweder neu oder zum Nachrüsten.

Stromausfall

Die „Elektronischer Schließzylinder“ beziehen die notwendige Energie über mitgelieferte Batterien.

- Die „Elektronischer Schließzylinder“ sind unabhängig eingesetzt:
 - Die „Elektronischer Schließzylinder“ funktionieren weiter.
- Die „Elektronischer Schließzylinder“ sind in einem System integriert:
 - Die „Elektronischer Schließzylinder“ funktionieren weiter, das System nicht.

1.4 Busch-AccessControl und smartIP

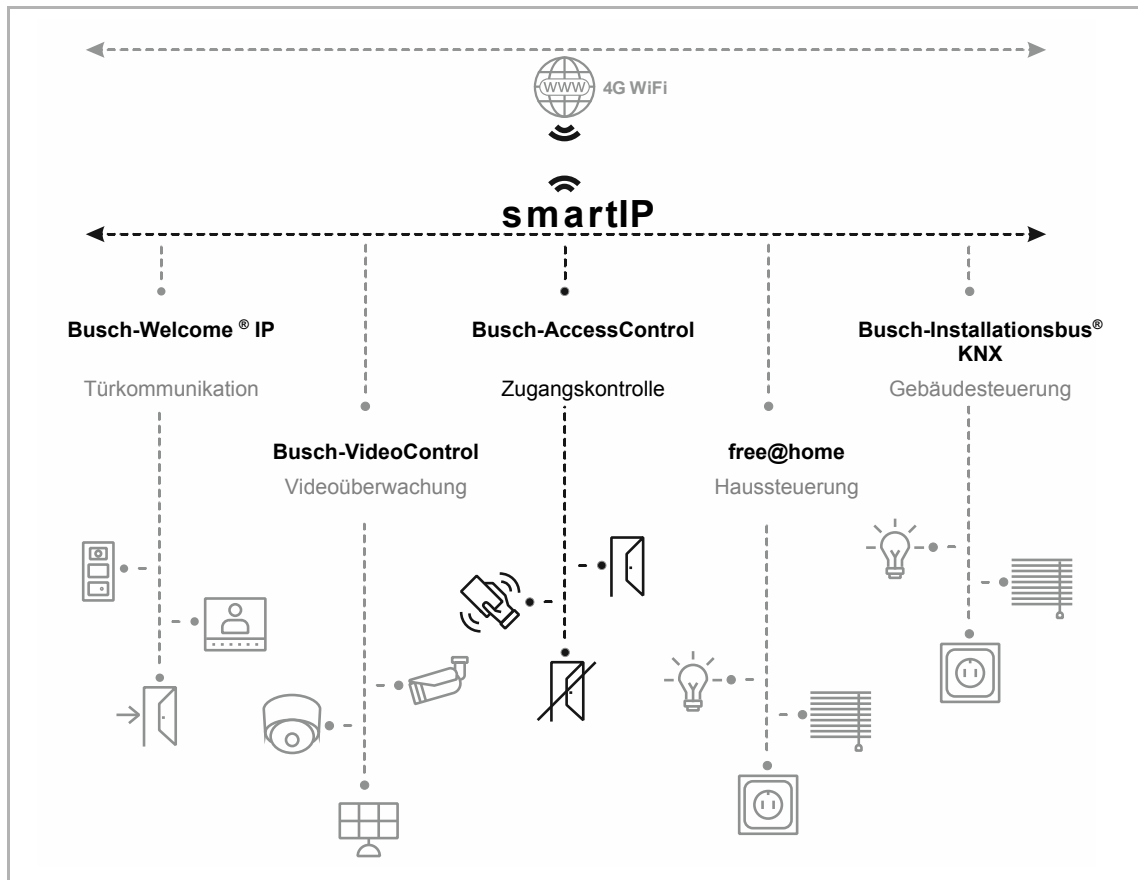


Abb. 1: Busch-AccessControl und smartIP

Das Zugangssystem Busch-AccessControl ist Bestandteil des Gesamtsystems smartIP.

Das Zugangssystem Busch-AccessControl kann allein für sich verwendet werden. Ebenso lässt es sich, je nach Wunsch, um die weiteren Systeme ergänzen oder zusätzlich in diese integrieren. Dies kann auch später zu einem beliebigen Zeitpunkt erfolgen.

Für die Planung gibt es für jedes System ein gesondertes Systemhandbuch.

1.5 Grundlagen strukturierter Verkabelung

Eine strukturierte Verkabelung ist ein einheitlicher Aufbauplan für eine Netzwerkinfrastruktur. Die Netzwerkinfrastruktur ist anwendungsunabhängig und zukunftsorientiert. Weitere Bezeichnungen für die strukturierte Verkabelung sind die Universelle Gebäudeverkabelung (UGV) oder Universelle Kommunikationsverkabelung (UKV).

Eine strukturierte Verkabelung soll teure Fehlinstallationen und Erweiterungen vermeiden und ebenso die Installation neuer Netzwerkkomponenten erleichtern.

Unstrukturierte Verkabelungen sind im Normalfall an den Bedarf oder an eine bestimmte Anwendung gebunden. Wird die Umstellung auf eine neue Technik oder Technik-Generation erforderlich, führt dies schnell zu einer Kostenexplosion.

Eine strukturierte Verkabelung basiert auf einer allgemeingültigen Verkabelungsstruktur. Diese Verkabelungsstruktur berücksichtigt unter anderem die Anforderungen für mehrere Jahre in die Zukunft. Sie enthält Reserven und lässt sich unabhängig von der Anwendung nutzen. Z. B. lässt man das lokale Netzwerk und die Telefonie über dieselbe Verkabelung laufen.

Eine strukturierte Verkabelung beinhaltet die folgenden Punkte:

- standardisierte Komponenten (Leitungen, Steckverbindungen, ...)
- hierarchische Netzwerk-Topologie (Stern, Baum, ...)
- Empfehlungen für Verlegung und Installation
- standardisierte Mess-, Prüf- und Dokumentationsverfahren

Ziele einer strukturierten Verkabelung

- Unterstützung aller heutigen und zukünftigen Kommunikationssysteme
- Kapazitätsreserve hinsichtlich der Grenzfrequenz
- Neutrales Verhalten des Netzes gegenüber dem Übertragungsprotokoll und den Endgeräten
- flexible Erweiterbarkeit
- Ausfallsicherheit durch sternförmige Verkabelung
- realisierbarer Datenschutz und Datensicherheit
- Einhaltung existierender Standards

Normen für die strukturierte Verkabelung

Geltungsbereich	Norm	Beschreibung
Europa	EN 50173-1 (2003)	Verkabelungsnorm Informationssystem - anwendungsneutrale Verkabelungssysteme
Nordamerika	TIA/EIA 568 B.1 (2001) / B.2 1 (2001)	Telekommunikations-Verkabelungsnorm für Gebäudeverkabelungen
Welt	ISO/IEC 11801 (2002)	Verkabelungsnorm für anwendungsneutrale Gebäudeverkabelungen

Tab. 1: Normen strukturierte Verkabelung

ISO/IEC 11801 (2002) und EN 50173-1 (2003)

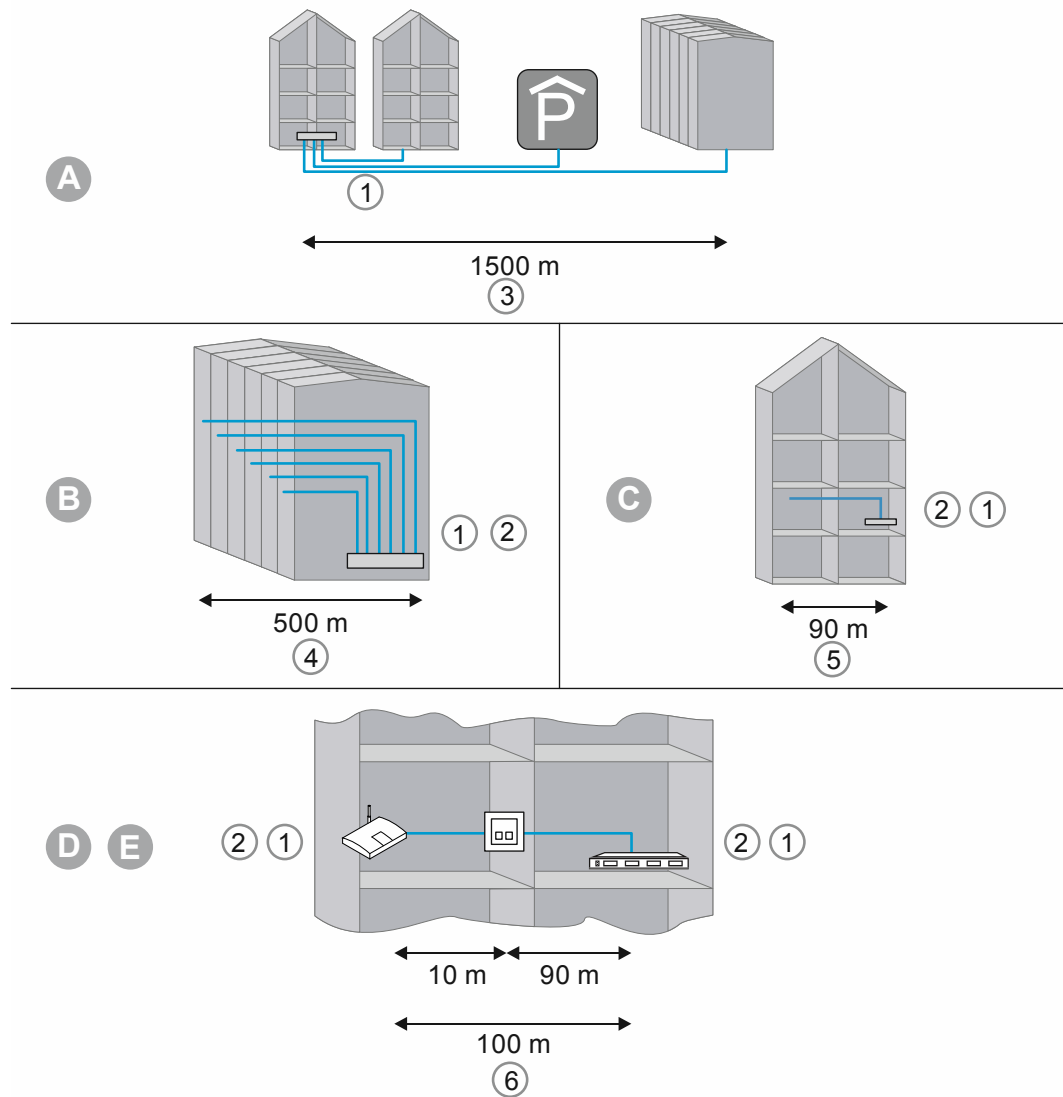


Abb. 2: Strukturierte Verkabelung

A	Standortverteiler
B	Gebäudeverteiler
C	Etagenverteiler
D	Anschlussdose
E	Endgerät
1	Lichtwellenleiter
2	Kupferleiter
3	Primärbereich
4	Sekundärbereich
5	Tertiärbereich
6	Tertiärbereich inklusive Patchkabel

Tab.2: Strukturierte Verkabelung

In der Europa-Norm (EN) und dem weltweit gültigen ISO-Standard erfolgt die Strukturierung in Form von Hierarchieebenen. Diese Ebenen werden von Gruppen gebildet. Diese Gruppen gehören topologisch oder administrativ zusammen.

Die Verkabelungen sind in die folgenden Bereiche gegliedert:

- Geländeverkabelung (Primärverkabelung)
- Gebäudeverkabelung (Sekundärverkabelung)
- Etagenverkabelung (Tertiärverkabelung)

Die Verkabelungsstandards sind für die folgende geografische Ausdehnung optimiert:

- Ausdehnung: 3000 m,
- Fläche: 1.000.000 qm
- Anwender: 50 ... 50.000

In jedem Verkabelungsbereich sind maximal zulässige Kabellängen festgelegt und müssen bei der Installation eingehalten werden. Viele Übertragungstechniken beziehen sich auf die definierten Kabellängen und Qualitätsanforderungen.



Hinweis

Alle ISO-Standards sind Handlungsempfehlungen. Die Einhaltung einer ISO-Norm ist freiwillig. Die Einhaltung der ISO-Standards wird im Normalfall von verschiedenen Seiten, zum Beispiel Kooperationspartnern, Herstellern und Kunden, gefordert.

Primärverkabelung - Geländeverkabelung

Der Primärbereich wird als Campusverkabelung oder Geländeverkabelung bezeichnet. Der Primärbereich realisiert die Verkabelung von einzelnen Gebäuden untereinander. Der Primärbereich umfasst meist große Entfernungen, hohe Datenübertragungsraten sowie eine geringe Anzahl von Stationen.

Für die Verkabelung wird in den meisten Fällen Glasfaserkabel (50 µm) mit einer maximalen Länge von 1.500 m verwendet. Im Normalfall sind dies Glasfaserkabel mit Multimodefasern oder bei größeren Entfernungen ebenfalls Glasfaserkabel mit Singlemodefasern. Für kleinere Entfernungen werden gelegentlich ebenfalls Kupferkabel verwendet.

Der Primärbereich sollte grundsätzlich großzügig geplant werden. Das Übertragungsmedium soll bezüglich der Bandbreite und der Übertragungsgeschwindigkeit nach oben hin offen sein. Dies gilt ebenfalls für das eingesetzte Übertragungssystem. Als Faustregel gilt 50 Prozent Reserve zum derzeitigen Bedarf der Investition.

Sekundärverkabelung - Gebäudeverkabelung

Der Sekundärbereich wird als Gebäudeverkabelung oder Steigbereichverkabelung bezeichnet. Der Sekundärbereich realisiert die Verkabelung von einzelnen Etagen und Stockwerken untereinander innerhalb eines Gebäudes. Dazu sind vorzugsweise Glasfaserkabel (50 µm) oder Kupferkabel mit einer maximalen Länge von 500 m vorgesehen.

Tertiärverkabelung - Etagenverkabelung

Der Tertiärbereich wird als Etagenverkabelung bezeichnet. Der Tertiärbereich realisiert die Verkabelung von Etagen- oder Stockwerksverteiltern zu den Anschlussdosen. Während sich im Stockwerksverteiler ein Netzwerkschrank mit Patchfeld befindet, mündet das Kabel am Arbeitsplatz des Anwenders in einer Anschlussdose in der Wand, in einem Kabelkanal oder in einem Bodentank mit Auslass.

Für diese relativ kurze Strecke werden Twisted-Pair-Kabel verwendet, deren Länge auf insgesamt 100 m (90 m plus 2x 5 m Anschlusskabel) begrenzt ist. Alternativ werden ebenfalls Glasfaserkabel (62,5 µm) eingesetzt.

Bestandteile der strukturierten Verkabelung:

- Patchfeld (Patchpanel)
- Patchkabel
- Anschlussdosen
- Netzwirkabel
- Verteilerschränke
- Switch, Hubs, Router

1.6 Designlinien

Dieses Systemhandbuch dient der technischen Planung einfacher bis komplexer Installationen.

Die unterschiedlichen Designlinien (mit den jeweiligen besonderen Farben und Formen der Geräte) sind in diesem Systemhandbuch nicht aufgeführt.

Bitte entnehmen Sie die gewünschten aktuellen Designvarianten und die entsprechenden vollständigen Artikelnummern sowie die Bestellnummern den jeweiligen Produktkatalogen oder dem Online-Katalog unter <https://busch-jaeger-katalog.de>

1.7 Grundlagen

Informationen über grundlegende Funktionen und Arbeitsweisen der Geräte finden Sie unter Kapitel 4 „Planungs- / Anwendungsinformationen“ auf Seite 54.

2 Sortimentsübersicht

2.1 Einsatz

Die batteriebetriebenen Zugangsgeräte des „Busch-AccessControl“ sind grundsätzlich für den Einsatz in einem IP-System vorgesehen. Für die Verwaltung der batteriebetriebenen Zugangsgeräte ist ein „Smart Access Point Pro“ erforderlich. In der Verwaltungssoftware des „Smart Access Point Pro“ werden die batteriebetriebenen Zugangsgeräte und Transponderschlüssel sowie Zugangsberechtigungen für Personen verwaltet.

Die lokale Kommunikation der batteriebetriebenen Zugangsgeräte erfolgt über Bluetooth. Das System „Busch-AccessControl“ kann eigenständig betrieben oder über dem „Smart Access Point Pro“ mit weiteren Systemen, z.B. Busch-Welcome[®] IP oder dem Heimnetzwerk vernetzt sein. Auf diesem Weg werden die batteriebetriebenen Zugangsgeräte Teil des Smart Home. Eine App-Steuerung über ein Smartphone ist dann ebenfalls möglich.

2.2 Anwendungsbereiche

Anwendungsbereiche von kabellosen Zugangssystemen

Mögliche Zugänge

Zugänge	
<ul style="list-style-type: none"> ▪ Zugangstüren ▪ Server- und Racktüren <ul style="list-style-type: none"> – Nur bei vorgesehenem Einbau von Schließzylindern 	<ul style="list-style-type: none"> ▪ Maschinentüren ▪ Aufzüge

Tab.3: Zugänge

Anwendungsbereiche	
PRIVATHÄUSER	
INDUSTRIE und GEWERBE	
<ul style="list-style-type: none"> ▪ Bürogebäude 	<ul style="list-style-type: none"> ▪ Industriegebäude
EINZELHANDEL	
BILDUNGSWESEN	
<ul style="list-style-type: none"> ▪ Universitäten ▪ Studentenwohnheime ▪ Akademien 	<ul style="list-style-type: none"> ▪ Schulen ▪ Forschungsinstitute ▪ Kindergärten
GESUNDHEITSWESEN	
<ul style="list-style-type: none"> ▪ Krankenhäuser ▪ Pflegeheime ▪ Betreutes Wohnen 	<ul style="list-style-type: none"> ▪ Spitäler ▪ Ambulante Pflegedienste
ÖFFENTLICHE EINRICHTUNGEN	
<ul style="list-style-type: none"> ▪ Parlamente ▪ Rathäuser ▪ Polizeipräsidien ▪ Militäranlagen 	<ul style="list-style-type: none"> ▪ Ministerien ▪ Ämter und Verwaltungen ▪ Justizeinrichtungen
LOGISTIK	
<ul style="list-style-type: none"> ▪ Flughäfen ▪ Häfen ▪ Logistikzentren 	<ul style="list-style-type: none"> ▪ Bahnhöfe ▪ Schiffe ▪ Lager
HOTELLERIE	
<ul style="list-style-type: none"> ▪ Design- und Luxushotels ▪ Familienhotels 	<ul style="list-style-type: none"> ▪ Businesshotels ▪ Ferienanlagen
FREIZEIT und UNTERHALTUNG	
<ul style="list-style-type: none"> ▪ Stadien ▪ Kinos und Theater ▪ Bäder ▪ Restaurants 	<ul style="list-style-type: none"> ▪ Fitnessklubs ▪ Freizeitparks ▪ Museen ▪ Sportzentren

Tab.4: Anwendungsbereiche

2.3 Geräteübersicht

2.3.1 Aufbau der Artikelnummern

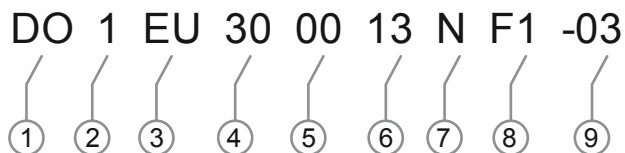


Abb. 3: Übersicht Artikelnummern

Nr.	Bedeutung		
1	System:	▪ DO	Busch-AccessControl
2	Gerätetyp:	▪ 1 ▪ 2 ▪ 5 ▪ 6 ▪ 8 ▪ 9	Schließzylinder Reserviert für: Beschlag Reserviert für: Wandler Reserviert für: Tür-Kontroller Zubehör Ersatzteil
3	Profiltyp	▪ EU	Europa
4	Zylinderlänge Tür-Außenseite	▪ XX	In mm
5	Zylinderlänge Tür-Innenseite	▪ XX	In mm
6	Abstand (zwischen Leseknauf und Zylindermechanik)	▪ 3 ▪ 8 ▪ 13	3 mm Reserviert für: 8 mm Reserviert für: 13 mm
7	Endstück	▪ T ▪ K ▪ N	Drehknauf Elektronischer Lesekopf Kein Endstück
8	Oberflächen	Lesekopf: ▪ F1 ▪ F2 ▪ F3	CSB (Chrome-Satin-Black) CWS (Reserviert) PPB (Reserviert)
		Transponderschlüssel: ▪ C1 ▪ C2 ▪ C3	Grau Weiß (Reserviert) Blau (Reserviert)
9	Marke	▪ -03	Busch-Jaeger

2.3.2 Schließzylinder

Schließzylinder für Europa: Profil EU

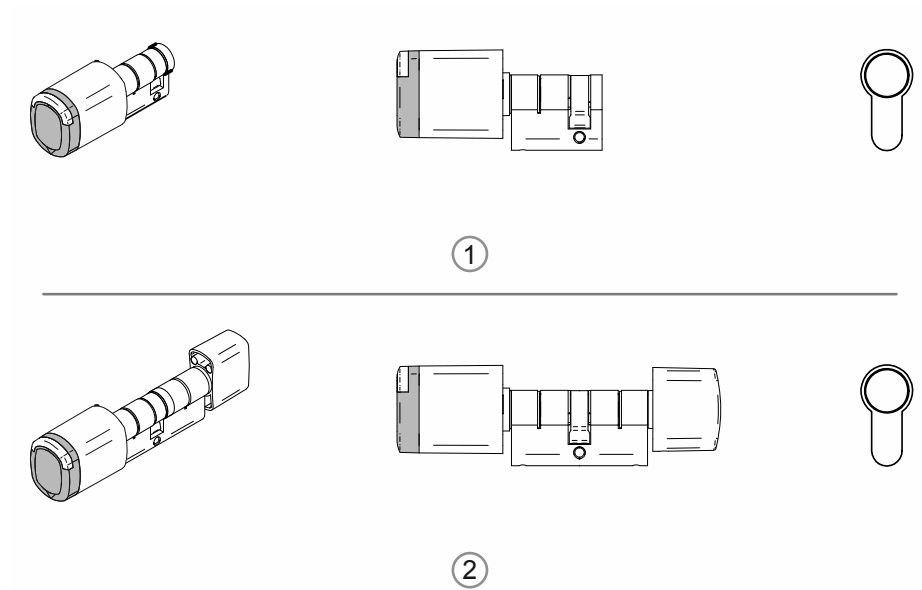


Abb. 4: Schließzylinder Profil EU

Nr.	Schließzylinder
[1]	Halbzylinder mit Lesekeyhole
[2]	Doppelzylinder mit Lesekeyhole und Handkeyhole

2.3.3 Systemgeräte

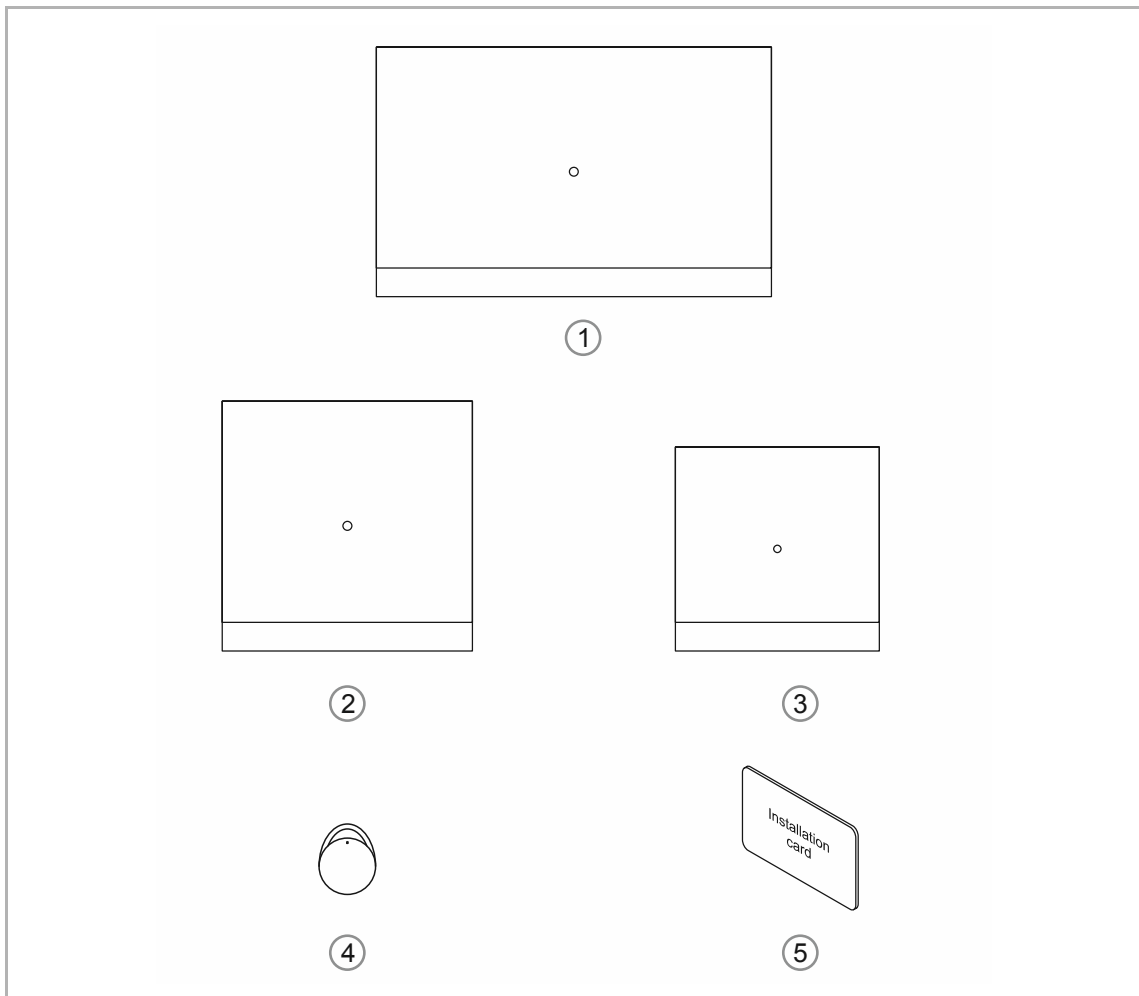


Abb. 5: Systemgeräte

[1] „Smart Access Point Pro“ D04011

Auf dem „Smart Access Point Pro“ ist die Managementsoftware installiert.

Der „Smart Access Point Pro“ bietet den Zugangspunkt, um mit dem PC oder mobilen Endgeräten die „Busch-AccessControl“ Anlage in Betrieb zu nehmen und zu verwalten.

Zum Öffnen der webbasierten Benutzeroberfläche des „Smart Access Point Pro“ benötigen Sie einen Computer mit LAN- oder WLAN-Netzwerkadapter und installiertem Internet-Browser.

Der „Smart Access Point Pro“ hat die folgenden Hauptfunktionen:

- Direktes Ansteuern von bis zu 16 „Elektronischer Schließzylinder“.
- Verwalten von bis zu 600 „Elektronischer Schließzylinder“ in der „Busch-AccessControl“ Anlage
- Spannungsversorgung über PoE oder separaten Spannungsnetzteil.

[2] RF/IP Gateway

Der RF/IP Gateway erweitert die Ansteuerungskapazität des „Smart Access Point Pro“ zu den „Elektronischer Schließzylinder“. An einen „Smart Access Point Pro“ lassen sich bis zu 64 RF/IP Gateway anbinden. Die Anbindung erfolgt über einen PoE-Switch.

Der RF/IP Gateway hat die folgenden Hauptfunktionen:

- Ansteuern von bis zu 16 „Elektronischer Schließzylinder“.
- Weiterleiten der Kommunikation zwischen den angesteuerten „Elektronischer Schließzylinder“ und dem dem „Smart Access Point Pro“.
- Spannungsversorgung über PoE oder separaten Spannungsnetzteil.

[3] Repeater

Der Repeater erhöht die Funkreichweite des „Smart Access Point Pro“ oder eines RF/IP Gateway zu den „Elektronischer Schließzylinder“. An einen „Smart Access Point Pro“ oder einen RF/IP Gateway lassen sich bis zu 3 Repeater in einer Linie hintereinanderschalten.

Die Funkreichweite zwischen den Geräten beträgt maximal etwa 10 Meter.

Der RF/IP Gateway hat die folgenden Hauptfunktionen:

- Weiterleiten der Kommunikation von bis zu 16 „Elektronischer Schließzylinder“.
- Spannungsversorgung über separates Spannungsnetzteil.

[4] Transponderschlüssel

Mit dem Transponderschlüssel werden die „Elektronischer Schließzylinder“ bedient.

Die Transponderschlüssel sind fertig vorkonfiguriert und betriebsbereit.

Die Personalisierung der Transponderschlüssel erfolgt in der Verwaltungssoftware des „Smart Access Point Pro“ in drei Schritten:

- Dem Transponderschlüssel werden die Türen zugewiesen, die dieser öffnen darf.
- Einem Benutzer wird ein Transponderschlüssel zugewiesen, den dieser benutzen darf.
- Einem Benutzer werden die Räume zugewiesen, die dieser öffnen darf.

Über die Kommunikation des „Elektronischer Schließzylinder“ mit der Verwaltungssoftware des „Smart Access Point Pro“ wird dann einem Benutzer das Öffnen einer Tür gestattet oder nicht gestattet.

[5] Installationskarte

Mit der Installationskarte werden die Leseköpfe der „Elektronischer Schließzylinder“ in Betrieb genommen.

- Für die Inbetriebnahme muss zwischen dem Lesekopf eines „Elektronischer Schließzylinder“ und dem „Smart Access Point Pro“ eine Funkverbindung bestehen.

2.3.4 Zubehör

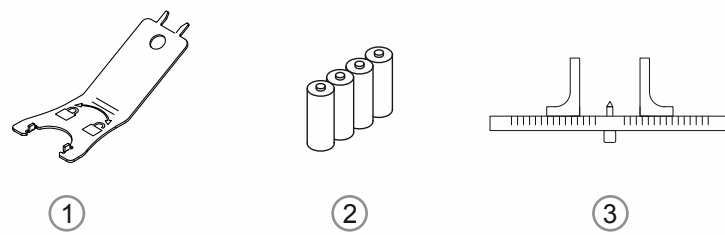


Abb. 6: Zubehör

1	Montagewerkzeug	Artikelnummer: D080MT-03
2	Batterien (handelsüblich)	<ul style="list-style-type: none"> ▪ Bei jedem „Elektronischer Schließzylinder“ liegt ein Satz Batterien (4x LR1) bei. <ul style="list-style-type: none"> – Dieser Satz hält bei normalem Gebrauch etwa 2 ... 3 Jahre. – Dieser Satz hält bei normalem Gebrauch bis etwa 110.000 Betätigungen. ▪ Für den Austausch werden handelsübliche LR1 Batterien verwendet.
3	Messlehre für Schließzylinder (handelsüblich)	<p>Zur Erleichterung des Ausmessens von Türbreiten bietet der Handel verschiedene Formen von Messlehren an.</p> <ul style="list-style-type: none"> – Spezielle Messlehren sind für das Ausmessen der Türbreiten jedoch nicht zwingend erforderlich.

2.4 Montagemöglichkeiten

2.4.1 Voraussetzungen

Sicherheitsbeschläge

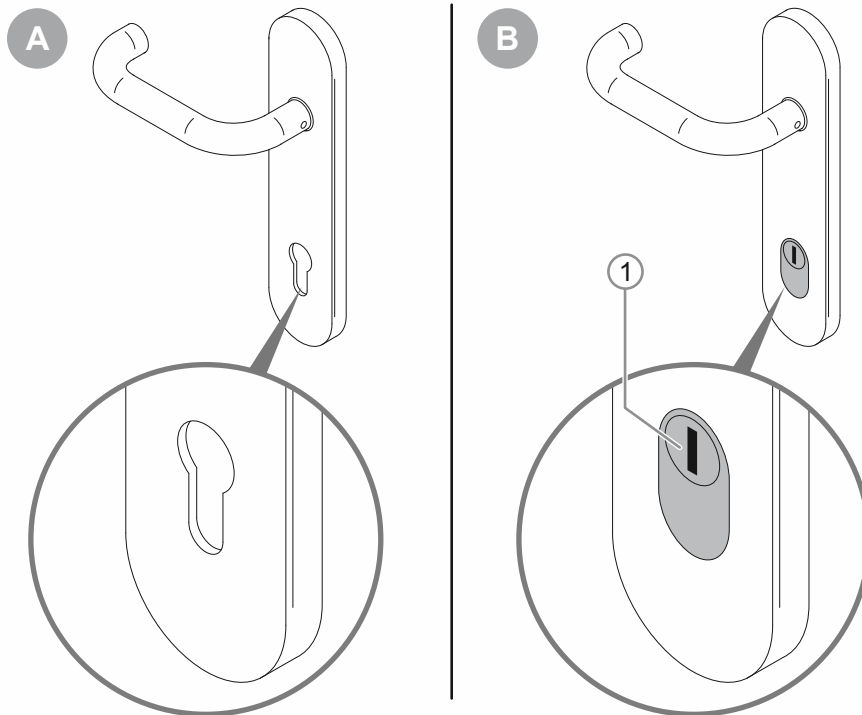


Abb. 7: Montagesituation Sicherheitsbeschläge

[A]: Standard-Türbeschlag

- Montage des „Elektronischer Schließzylinder“ möglich.

[B]: Türsicherheitsbeschlag mit Kernziehschutz / Zylinderschutz

- Montage des „Elektronischer Schließzylinder“ prüfen.
 - Lässt sich die Zylinderabdeckung [1] aus dem Türsicherheitsbeschlag entnehmen, ist eine Montage eventuell möglich.
 - Ist eine Montage des „Elektronischer Schließzylinder“ nicht möglich, muss der Türbeschlag getauscht werden.

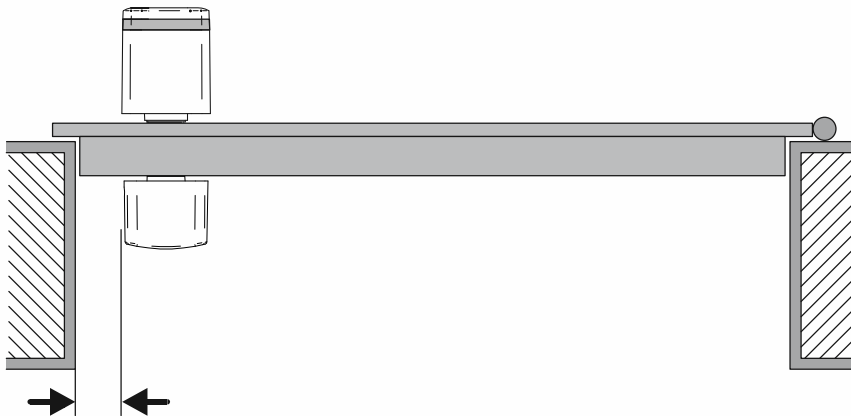
Platzverhältnisse

Abb. 8: Montagesituation Platzverhältnisse

Für die Montage des „Elektronischer Schließzylinder“ muss ausreichend Platz zum Türrahmen vorhanden sein. Nach der Montage des „Elektronischer Schließzylinder“ sollte man den Knauf noch mit den Fingern umgreifen können. Für die kalte Jahreszeit oder in Kühlbereichen auch mit Handschuhen.

2.4.2 Schließzylinder ausmessen

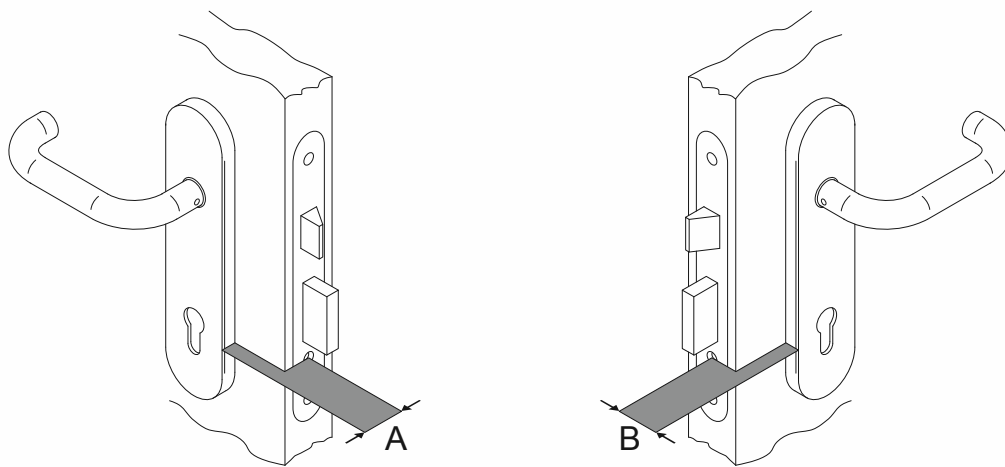


Abb. 9: Schließzylinder ausmessen: Türbreite

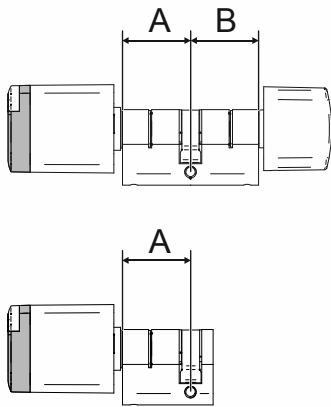


Abb. 10: Schließzylinder: Zylinderbreite Profil EU

		A								
		30	35	40	45	50	55	60	65	70
B	30	x*	x	x	x	x	x	x	x	x
	35	x*	x	x	x	x	x	x	x	x
	40	x	x*	x	x	x	x	x	x	x
	45	x	x	x*	x	x	x	x	x	x
	50	x	x	x*	x	x	x	x	x	x
	55	x	x	x	x	x	x	x	x	x
	60	x	x	x	x	x	x	x	x	x
	65	x	x	x	x	x	x	x	x	x
	70	x	x	x	x	x	x	x	x	x

Tab. 5: Längen in Millimeter

* : Standardgrößen

- Standardgrößen sind sofort lieferbar.
- Alle andern Größen haben eine zusätzliche Lieferzeit von 4 Wochen.

2.4.3 Alte Schließzylinder demontieren

Neben den ortsüblichen Standardzylindern werden ebenfalls andere Zylindersysteme eingesetzt, wenn die Situation dies erfordert. Müssen für den Einsatz des „Busch-AccessControl“ alte Schließzylinder entfernt werden, finden Sie im Folgenden Informationen über die Demontage von gängigen Schließzylindern.

Demontage Altzylinder: Profil Europa (EU) und Schweiz (CH)

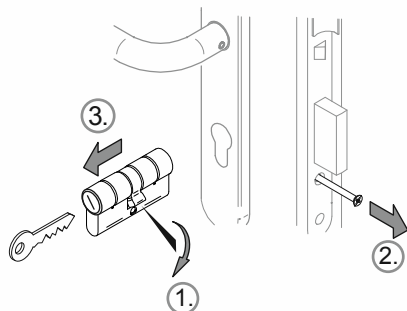


Abb. 11: Demontage Altzylinder: Profil Europa (EU) und Schweiz (CH)

Führen Sie zum Demontieren des vorhandenen Altzylinders die folgenden Punkte durch:

1. Den Mitnehmer senkrecht nach unten drehen.
2. Die Stulpschraube herausdrehen.
3. Den Zylinder entnehmen.

Demontage Altzylinder: Profil Skandinavian Oval

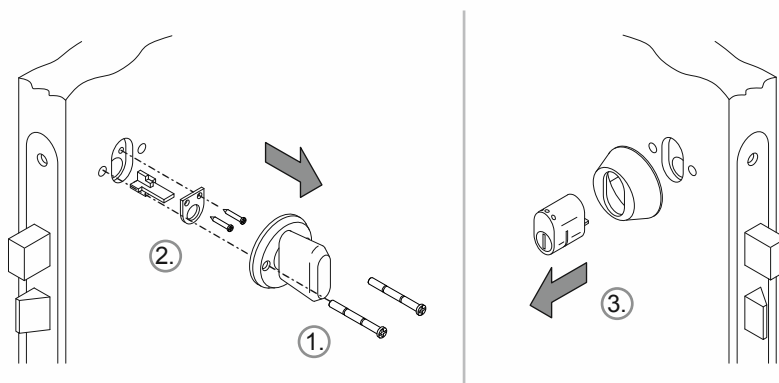


Abb. 12: Demontage Altzylinder: Profil Skandinavian Oval

Führen Sie zum Demontieren des vorhandenen Altzylinders die folgenden Punkte durch:

1. Auf der Innenseite den Knauf demontieren.
2. Auf der Innenseite das Montageset des Schließzylinders demontieren.
3. Auf der Außenseite den Zylinder entnehmen.

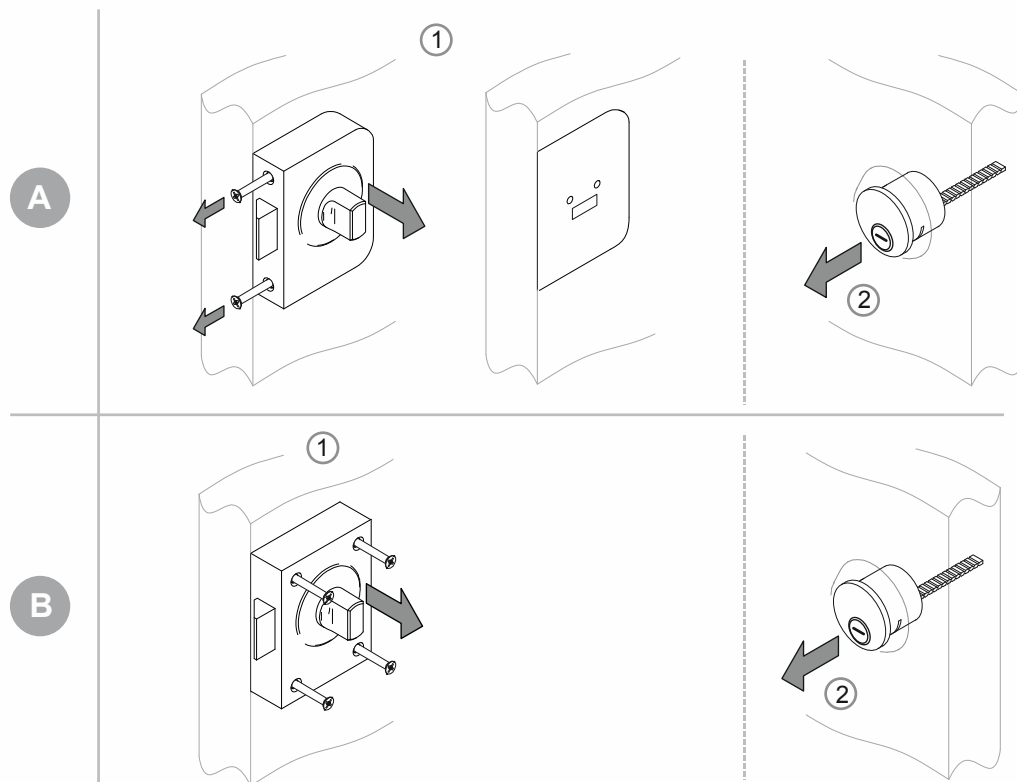
Demontage Altzylinder: Profil RIM

Abb. 13: Demontage Altzylinder: Profil RIM

Bei dem Zylinderprofil „RIM“ existieren zwei Grundarten von Schlössern.

[A] Mit Korpus und separater Grundplatte

[B] Kompletter Schlosskörper

[A]

1. Die seitlichen Schrauben herausdrehen und den Schlosskörper abnehmen.
 - Die Grundplatte verbleibt an ihrem Platz.
2. Den Schließzylinder entfernen.

[B]

1. Die Schrauben herausdrehen und das gesamte Schloss abnehmen.
2. Den Schließzylinder entfernen.

Demontage Altzylinder: Profil Mortise

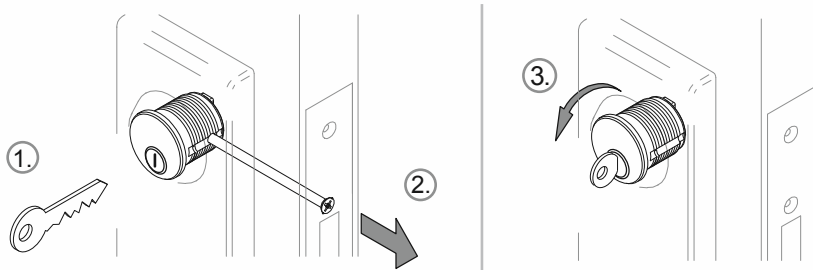


Abb. 14: Demontage Altzylinder: Profil Mortise

1. Den Schlüssel einstecken.
2. Die Feststellschraube soweit lösen, dass sich der Zylinder drehen lässt.
3. Den Zylinder mithilfe des Schlüssels herausdrehen.

3 Inbetriebnahme

3.1 Übersicht der Inbetriebnahme

Bei der Inbetriebnahme wird unterschieden zwischen der Inbetriebnahme der Systemgeräte („Smart Access Point Pro“, RF/IP-Gateway und Repeater) und dem Hinzufügen und Inbetriebnehmen von „Elektronischer Schließzylinder“.

Ist der „Smart Access Point Pro“ oder die Gebäudestruktur bereits vorhanden, z.B. in einem System „Busch-Welcome® IP“, entfällt dieser Teil der Inbetriebnahme. Die weiteren Schritte können direkt in der Verwaltungssoftware des „Smart Access Point Pro“ durchgeführt werden.

Schritt 1	Erstinbetriebnahme „Smart Access Point Pro“	siehe Kapitel 3.1.4 „„Smart Access Point“ in Betrieb nehmen“ auf Seite 34
Schritt 2	Gebäudestruktur erstellen	siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95
Schritt 3	Hinzufügen von „Smart Access Point Pro“	<ul style="list-style-type: none"> ▪ „Smart Access Point Pro“ in der Gebäudestruktur der Verwaltungssoftware hinzufügen: <ul style="list-style-type: none"> – siehe Kapitel 5.4.1 „„Smart Access Point Pro“ platzieren“ auf Seite 104
Schritt 4	Inbetriebnahme von RF/IP-Gateways	siehe Kapitel 3.2.3 „„RF/IP Gateway““ auf Seite 47
Schritt 5	Inbetriebnahme von Repeatern	siehe Kapitel 3.2.4 „Repeater“ auf Seite 48
Schritt 6	Hinzufügen von „Elektronischer Schließzylinder“	<ul style="list-style-type: none"> ▪ „Elektronischer Schließzylinder“ in Betrieb nehmen: <ul style="list-style-type: none"> – siehe Kapitel 3.2.1 „„Elektronischer Schließzylinder““ auf Seite 43 ▪ „Elektronischer Schließzylinder“ in der Verwaltungssoftware des „Smart Access Point Pro“ hinzufügen: <ul style="list-style-type: none"> – „Elektronischer Schließzylinder“ ist bereits montiert: siehe Kapitel 5.2.2 „„Elektronischer Schließzylinder“ hinzufügen“ auf Seite 89 – „Elektronischer Schließzylinder“ ist noch nicht montiert: siehe Kapitel 3.2.2 „„Elektronischer Schließzylinder“ vorab hinzufügen“ auf Seite 47 ▪ „Elektronischer Schließzylinder“ koppeln (Funklinie bestimmen): <ul style="list-style-type: none"> – siehe Kapitel 5.4.4 „Elektronischer Schließzylinder mit Smart Access Point koppeln“ auf Seite 112 ▪ Schließrechte in der Verwaltungssoftware des „Smart Access Point Pro“ erstellen: <ul style="list-style-type: none"> – siehe Kapitel 5.5 „Benutzerverwaltung“ auf Seite 118

3.2 Voraussetzungen

„Elektronischer Schließzylinder“

- Jeder Leseknauf muss bei der Inbetriebnahme eine Funkverbindung zum „Smart Access Point Pro“ besitzen.
 - Diese Funkverbindung kann direkt oder über den Umweg über andere Geräte bestehen.
 - Der Verbindungsweg an ihrem späteren Einsatzort muss vor dem Einbau der Geräte an in der Verwaltungssoftware des „Smart Access Point Pro“ festgelegt werden.
- Alle „Elektronischer Schließzylinder“ können vor Ort gemeinsam in Betrieb genommen werden. Dazu müssen sich alle Geräte des Systems in der Nähe des „Smart Access Point Pro“ befinden. Nach der gemeinsamen Inbetriebnahme werden die Geräte dann an ihren Einsatzort montiert.

- Sind für den Einsatz der „Elektronischer Schließzylinder“ weitere Geräte notwendig (RF/IP-Gateways oder Repeater), müssten diese für die Inbetriebnahme der „Elektronischer Schließzylinder“ bereits in Betrieb genommen sein.

„Smart Access Point Pro“

Für den Einsatz des Systems „Busch-AccessControl“ ist ein „Smart Access Point Pro“ erforderlich.

- Ist eine andere Variante des „Smart Access Point“ bereits vorhanden und soll beibehalten werden, ist die Verwaltung des Systems „Busch-AccessControl“ zusammen mit einem nachgeschalteten RF/IP-Gateway möglich.
- Eine andere Variante eines „Smart Access Point“ kann das System „Busch-AccessControl“ ohne einen nachgeschalteten RF/IP-Gateway nicht verwalten.

RF/IP-Gateway

Repeater

3.1 Inbetriebnahme des Systems — „Smart Access Point Pro“

3.1.1 Übersicht

Die Inbetriebnahme des „Smart Access Point Pro“ erfolgt in 3 Teil-Abschnitten.

– Beachten Sie die Reihenfolge der Schritte. Diese hängen voneinander ab.

1.	„Smart Access Point Pro“ via WLAN mit einem Rechner verbinden und die Webseite des „Smart Access Point Pro“ aufrufen.	siehe Kapitel 3.1.2 „Einen PC mit dem „Smart Access Point“ Verbinden“ auf Seite 30
2.	Vorentscheidung über den Systemmodus treffen.	siehe Kapitel 3.1.3 „Vorabinformation: Auswahl der Systemmodi“ auf Seite 32
3.	Assistenten durchlaufen mit Auswahl des Systemmodus.	siehe Kapitel 3.1.4 „„Smart Access Point“ in Betrieb nehmen“ auf Seite 34

3.1.2 Einen PC mit dem „Smart Access Point“ Verbinden



Achtung! Datenverlust

Der „Smart Access Point“ bindet die gefundenen Geräte mit Hilfe von Zertifikaten in das System sicher ein. Dadurch ist eine verschlüsselte Kommunikation zwischen allen Geräten erst möglich.

- Führen Sie nach der Inbetriebnahme ein Backup durch.
 - Sollte der „Smart Access Point“ einmal defekt sein, müssten Sie ohne Backup ansonsten das gesamte System neu in Betrieb nehmen.

„Smart Access Point“ via WLAN mit dem PC verbinden

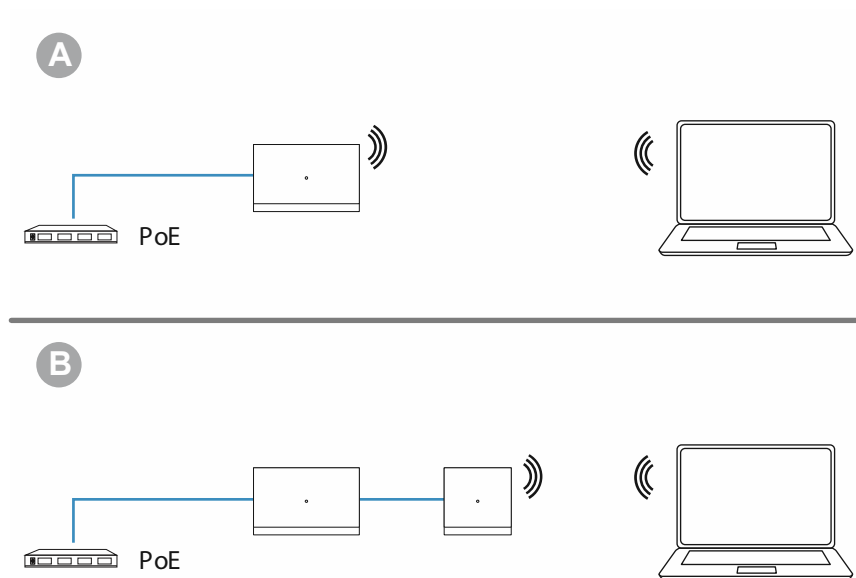


Abb. 15: „Smart Access Point“ mit PC verbinden (Access-Point Modus)

Sobald der „Smart Access Point“ über den PoE-Switch mit elektrischer Spannung versorgt wird, fährt das Gerät automatisch hoch.

- A: „Smart Access Point Pro“
- B: „Smart Access Point Lite“ mit nachgeschaltetem RF/IP-Gateway

Das Gerät befindet sich im Access-Point Modus (die LED leuchtet dauerhaft rot).

Führen Sie zum Verbinden mit dem PC die folgenden Schritte durch:

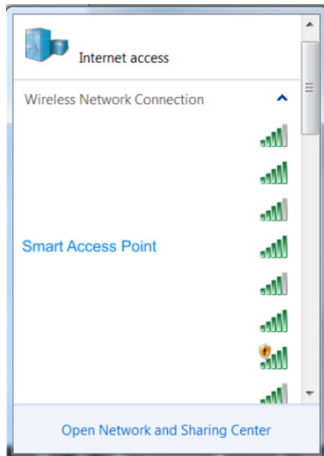


Abb. 16: „Smart Access Point“ in der Netzwerkliste des PC

1. Den PC mit dem WLAN des „Smart Access Point“ verbinden.
 - Die WLAN-Zugangsdaten befinden sich auf dem Gerät. Dazu die Abdeckung des Gerätes entfernen.

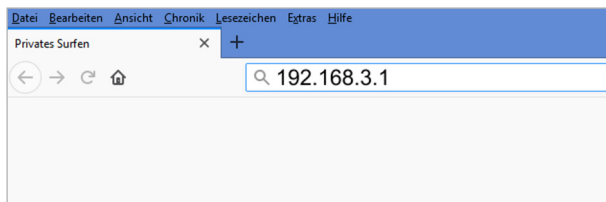


Abb. 17: IP-Adresse in einem Browser eingeben

2. In einem handelsüblichen Browser die Startseite des „Smart Access Point“ aufrufen.
 - Dafür die IP-Adresse „192.168.3.1“ in die Adresszeile des Browsers eingeben.

3.1.3 Vorabinformation: Auswahl der Systemmodi

Die Bedeutung des Betriebsmodus lässt sich am besten am Beispiel eines Busch-Welcome[®] IP Systems darstellen.

Auch wenn eine Integration weiterer Systeme nicht oder noch nicht vorgesehen ist, sollten Sie sich bereits jetzt Gedanken über die Auswahl des Systemmodus machen. Der Systemmodus kann im Nachhinein nicht mehr geändert werden.

Vorinformation Auswahl Systemmodi

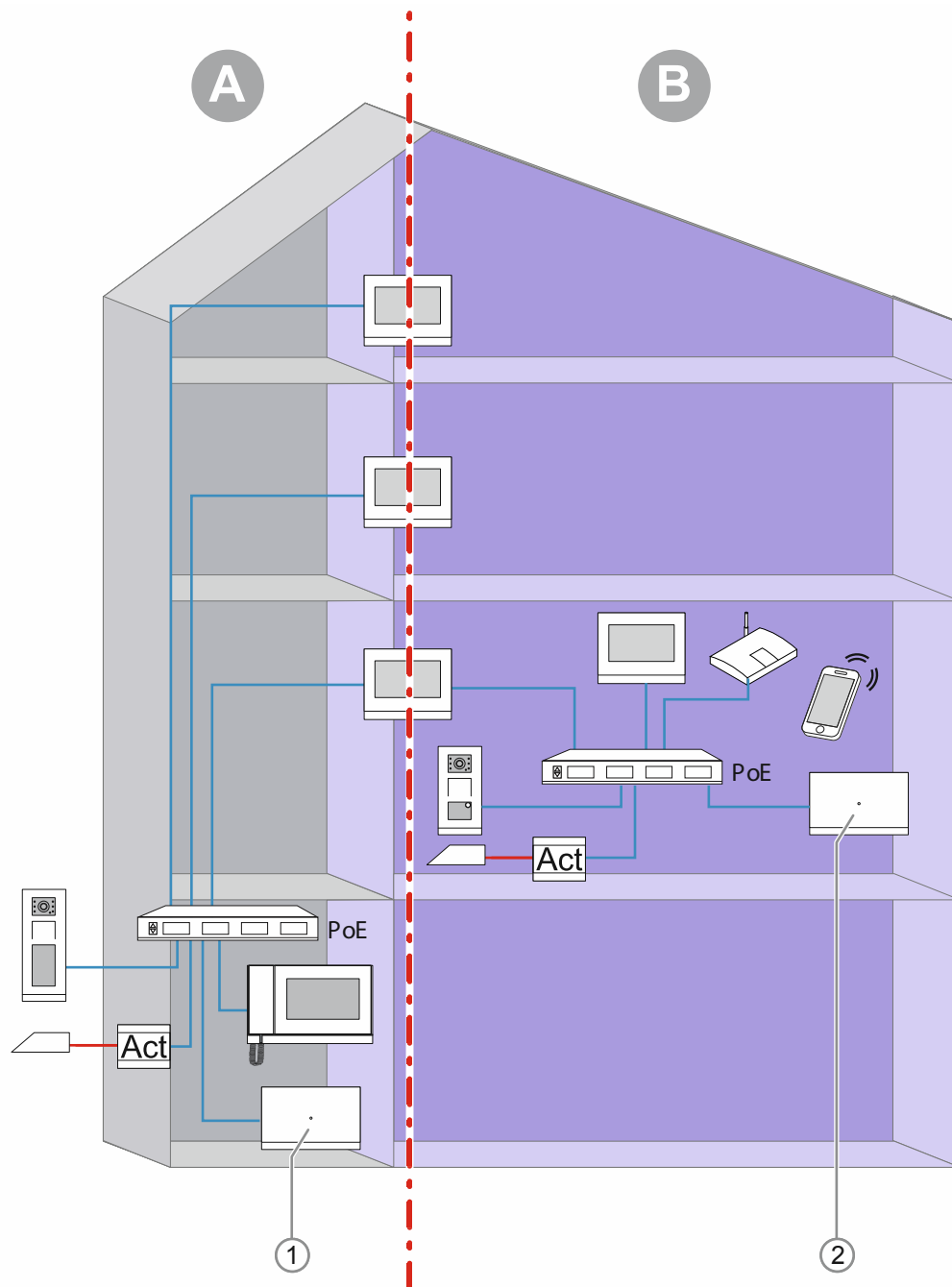


Abb. 18: Vorinformation Auswahl Systemmodi

In der Grafik sind zwei grundsätzliche Bereiche innerhalb von Gebäuden (hier ein

Wohngebäude) dargestellt. Beide Bereiche der Installation sind durch die erste Innenstation (Master) einer Einheit, die als IP-Gateway arbeitet, strikt voneinander getrennt. Keiner der Bereiche kann auf den anderen zugreifen.

- Bereich [A]: Der öffentliche Bereich (Gebäude-Netzwerk)
 - Hier empfängt z.B. der Concierge die Besucher und leitet die Besucher zu den einzelnen Wohnungen weiter. Auf die Installation hinter der 1. Innenstation der Wohnungen hat der Concierge keinen Zugriff.
- Bereich [B]: Der private Bereich (Einheiten-Netzwerk)
 - Dieser Bereich ist, wie der Name sagt, privat. Von dem öffentlichen Bereich kann auf das private Netzwerk hinter der 1. Innenstation nicht zugegriffen werden. Andersherum kann von dem privaten Bereich nicht auf den öffentlichen Bereich zugegriffen werden.
 - Möchte man einem Besucher den Haupteingang öffnen, geht dies nur über die 1. Innenstation. Die Türöffnerfunktion für den Haupteingang befindet sich „bildlich gesehen“ auf der Seite des öffentlichen Bereiches.
 - Möchte man den Eingang der Wohnung öffnen, lässt sich dies über alle Innenstationen und Smartphones (mit Busch-Welcome® App) der Wohnung durchführen.

Damit diese Sicherheit der Trennung erreicht wird, muss jeder der Bereiche von einem eigenen „Smart Access Point“ [1] / [2] gesteuert werden. Je nach dem Bereich, in dem der „Smart Access Point“ eingesetzt wird, erhält dieser einen entsprechenden Systemmodus.

In Gebäuden, in denen es nur einen Bereich gibt, können theoretisch beide Systemmodi zum Einsatz kommen. Dies sind z.B. reine Verwaltungsgebäude (nur Gebäude-Netzwerk) oder Einfamilienhäuser (nur Einheiten-Netzwerk). Um die Installation für zukünftige Erweiterungen offen zu halten, sollte trotzdem der passende Systemmodus gewählt werden.

Systemmodi des „Smart Access Point“

Für das spätere Hinzufügen der Geräte muss im Laufe der Schritte der Inbetriebnahme des „Smart Access Point“ bereits der Systemmodus bestimmt werden.

- Modus „Mehrparteienhaus / Gewerbe“:
 - Für ein Gebäude-Netzwerk.
 - Der „Smart Access Point“ befindet sich im Gebäude-Netzwerk.
 - Der „Smart Access Point“ hat die statische IP-Adresse „10.0.0.1“.
 - Über den 10er IP-Adressbereich wird mit den Busch-Welcome® IP Teilnehmern kommuniziert.
 - Parallel kann der „Smart Access Point“ per WLAN oder LAN mit einem Router verbunden werden und als DHCP-Client agieren. Dabei erhält das Gerät eine zusätzliche vom Router vergebene IP-Adresse. Diese nutzt er zusätzlich zu seiner eigenen 10er IP-Adresse.
- Modus „Einfamilienhaus / Reihenhaus“:
 - Für ein Einheiten-Netzwerk.
 - Der „Smart Access Point“ befindet sich im Einheiten-Netzwerk.
 - Der „Smart Access Point“ hat die statische IP-Adresse „10.0.0.1“.
 - Über den 10er IP-Adressbereich wird mit den Busch-Welcome® IP Teilnehmern kommuniziert.
 - Parallel kann der „Smart Access Point“ per WLAN oder LAN mit einem Router verbunden werden und als DHCP-Client agieren. Dabei erhält das Gerät eine zusätzliche vom Router vergebene IP-Adresse. Diese nutzt er zusätzlich zu seiner eigenen 10er IP-Adresse.

3.1.4 „Smart Access Point“ in Betrieb nehmen

Nachdem der „Smart Access Point“ mit dem PC verbunden ist und die Startseite des „Smart Access Point“ in dem Browser aufgerufen wurde, ist der „Smart Access Point“ bereit für die Inbetriebnahme.

Bei der Inbetriebnahme führt ein Assistent durch die einzelnen Schritte.

Führen Sie für die Inbetriebnahme des Gerätes die folgenden Schritte durch:

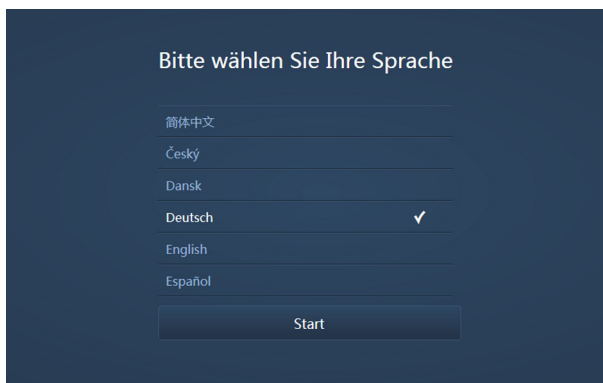


Abb. 19: Inbetriebnahme „Smart Access Point“: Landessprache

1. Die Landessprache auswählen.

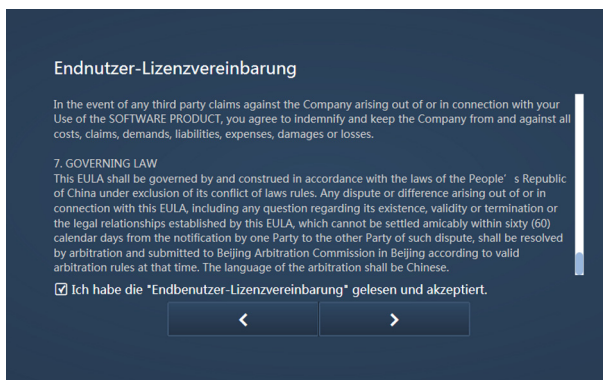


Abb. 20: Inbetriebnahme „Smart Access Point“: Lizenz-Vereinbarungen

2. Die folgenden Lizenz-Vereinbarungen akzeptieren:

- Endbenutzer Lizenz-Vereinbarung
- Software Lizenz-Vereinbarung
- Datenschutzerklärung

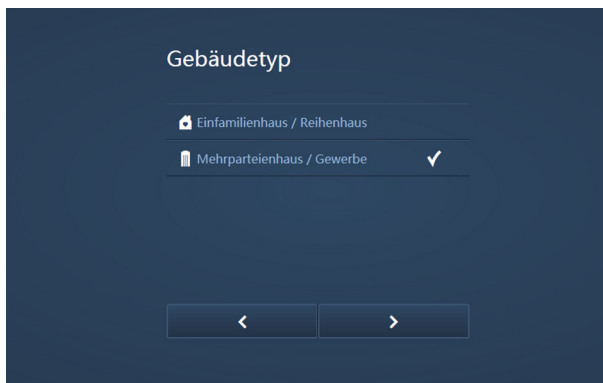


Abb. 21: Inbetriebnahme „Smart Access Point“: Gebäudetyp

3. Den Gebäudetyp (Systemmodus) auswählen.
 - Nähere Information: siehe Kapitel 3.1.3 „Vorabinformation: Auswahl der Systemmodi“ auf Seite 32.

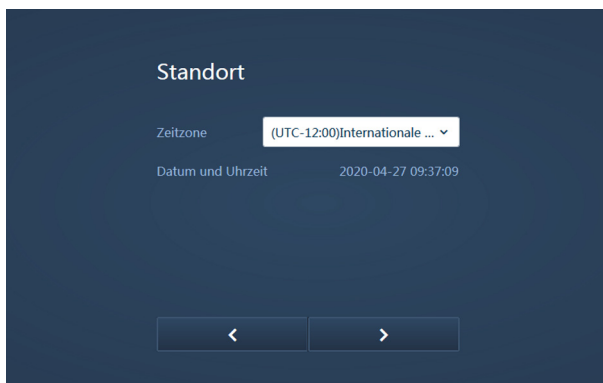


Abb. 22: Inbetriebnahme „Smart Access Point“: Standort

4. Den Standort eingeben.
 - Dieser Schritt lässt sich überspringen. Bei der späteren Wiederverbindung wird automatisch nach einem Abgleich gefragt, wenn die Werte zwischen dem PC und dem „Smart Access Point“ nicht übereinstimmen.



Abb. 23: Inbetriebnahme „Smart Access Point“: WiFi-Einstellungen

5. Die WiFi-Einstellungen des „Smart Access Point“ eingeben.
 - Name:

- Der Name ist frei wählbar. Dies kann z.B. der Name des Gerätes (befindet sich auf dem Gerät) oder der Gebäudename sein, in dem sich der „Smart Access Point“ befindet.
- Passwort:
 - Das Passwort ist später für jedes neue Aufrufen des „Smart Access Point“ notwendig.
 - Daran denken, sich das Passwort zu merken.
- Ländercode



Abb. 24: Inbetriebnahme „Smart Access Point“: Verbindung zum lokalen Netz

6. Verbindung zum lokalen Netz

- **Achtung! Diesen Schritt nicht überspringen.**
Für den Einsatz des „Smart Access Point“ im System Busch-Welcome® IP ist zwingend eine Auswahl der Verbindungsart notwendig. Auch, wenn keine Verbindung zu einem lokalen Netz geplant ist. Wird dieser Schritt übersprungen, lassen sich nach der Inbetriebnahme keine Geräte zum System hinzufügen.
- LAN: Bei geplanter Verbindung zum lokalen Netz über LAN
- WiFi: Bei geplanter Verbindung zum lokalen Netz über WLAN
- Ist keine Verbindung zu einem lokalen Netz geplant, eines der beiden auswählen.



Abb. 25: Inbetriebnahme „Smart Access Point“: Netzwerkeinstellungen

7. Netzwerkeinstellungen

- Aktivieren: IP-Adresse automatisch beziehen

- Die IP-Adressen der Geräte werden später beim Hinzufügen vom „Smart Access Point“ anhand der in den Geräten bereits eingestellten physikalischen Adressen generiert und verwaltet.
- Übrige Einstellungen so belassen.

Abb. 26: Inbetriebnahme „Smart Access Point“: Administratorkonto

8. Administratorkonto erstellen

- Das Administratorkonto besitzt Verwaltungs- und Änderungsrechte für das gesamte System. Zu einem späteren Zeitpunkt lassen sich noch weitere Konten hinzufügen. Z.B. ein Konto mit Rechten nur für die Schlüssel- und Namensverwaltung.

Abb. 27: Inbetriebnahme „Smart Access Point“: Optionen für Zurücksetzen

9. Optionen für das Zurücksetzen des „Smart Access Point“

- Für eine erhöhte Sicherheitsstufe kann die Option „Mit myBuildings-Konto“ gewählt werden.
 - Das Zugangspasswort für den „Smart Access Point“ kann dann nur mit einer Sicherheitsfreigabe, die per E-Mail über das „myBuildings-Konto“ versendet wird, zurückgesetzt werden.
 - Für diese Option ist die Registrierung für ein „myBuildings-Konto“ erforderlich.
 - Wenn Sie noch nicht für ein „myBuildings-Konto“ registriert sind, lässt sich dies für diese Auswahl im nächsten Schritt durchführen.

MyBuildings-Konto

Benutzername

Passwort

Klarname

Fernzugriff Aktivieren

Falls Sie noch keinen MyBuildings-Konto besitzen, können Sie sich hier [registrieren](#).

Abb. 28: Inbetriebnahme „Smart Access Point“: myBuildings-Konto

10. Daten für „myBuildings-Konto“ eingeben / Für „MyBuildingskonto“ registrieren

- Erforderlich, wenn im vorherigen Schritt die Option „Mit myBuildings-Konto“ gewählt wurde.
- Ist noch kein „myBuildings-Konto“ vorhanden, ist von hier aus eine Registrierung möglich [2].

Eindeutigen Gerätenamen definieren...

Gerätename

Abb. 29: Inbetriebnahme „Smart Access Point“: Gerätenamen

11. Eindeutigen Gerätenamen definieren

- Mit dem Gerätenamen wird der UPnP-Gerätenamen definiert.

Einstellungsübersicht

Sprache Deutsch

Haupttüröffner Default Lock

Zweiter Türöffner Subsidiary Lock

Zeitzone (UTC-12:00)Internation...

SSID SmartAP_EA58

Verbindungstyp L2

IP-Adresse

Abb. 30: Inbetriebnahme „Smart Access Point“: Einstellungsübersicht

12. Einstellungsübersicht

- Die Seite „Einstellungsübersicht“ ist eine reine Anzeige, in der alle vorgenommenen Einstellungen noch einmal überprüft werden können.
- Wenn sie mit dem Mauszeiger rechts neben den Text navigieren, wird ein Bildlauf eingeblendet.
- Soll eine Einstellung geändert werden, navigieren Sie über die Schaltflächen Vor / Zurück zur Seite mit den gewünschten Einstellungen und ändern diese. Die vorgenommenen Einstellungen der übrigen Seiten bleiben dabei erhalten.



Abb. 31: Inbetriebnahme „Smart Access Point“: Einstellungen bestätigen

13. Die vorgenommenen Einstellungen bestätigen.

- Das System konfiguriert sich.

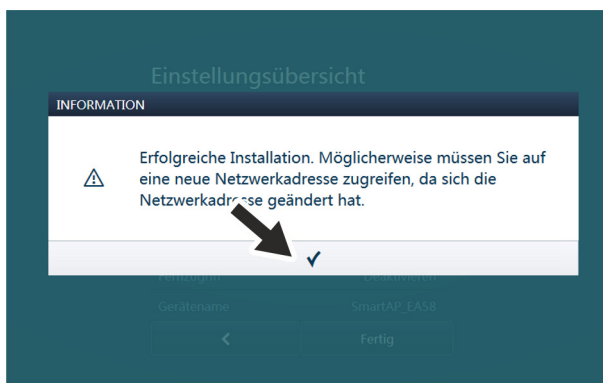


Abb. 32: Inbetriebnahme „Smart Access Point“: Inbetriebnahme bestätigen

14. Die Konfiguration bestätigen.

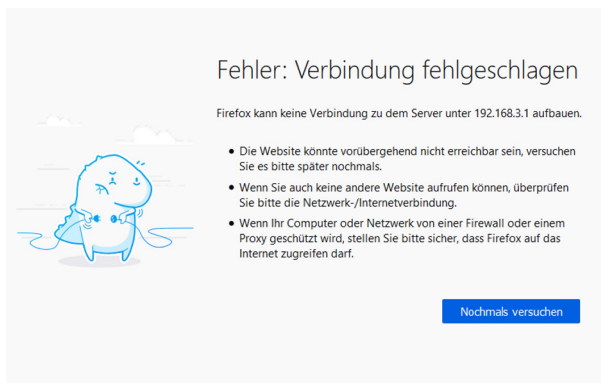


Abb. 33: Inbetriebnahme „Smart Access Point“: Verbindungstrennung

- Der „Smart Access Point“ schaltet am Ende der Erstinbetriebnahme automatisch in den Access-Point Modus (die LED leuchtet rot).
- Die WLAN-Verbindung mit dem „Smart Access Point“ wird automatisch getrennt und ist nicht mehr aktiv.
- Von nun an schaltet der „Smart Access Point“ direkt nach jedem Hochfahren automatisch in den Access-Point Modus.

Für die weiteren Schritte muss die Verbindung per LAN neu hergestellt werden. Die weiteren Schritte werden in den folgenden Kapiteln beschrieben.

3.1.5 Vorabinformation: IP-Adresse an einem PC angleichen

Je nach dem Systemaufbau muss die IP-Adresse der Verbindung auf dem PC / Laptop / etc. in denselben Bereich gebracht werden, wie die des Gerätes (nur einmal erforderlich). Der Webbrowser stellt ansonsten keine Verbindung zu dem Gerät her.

Einstellung der IP-Adresse am Beispiel Betriebssystem Windows 10

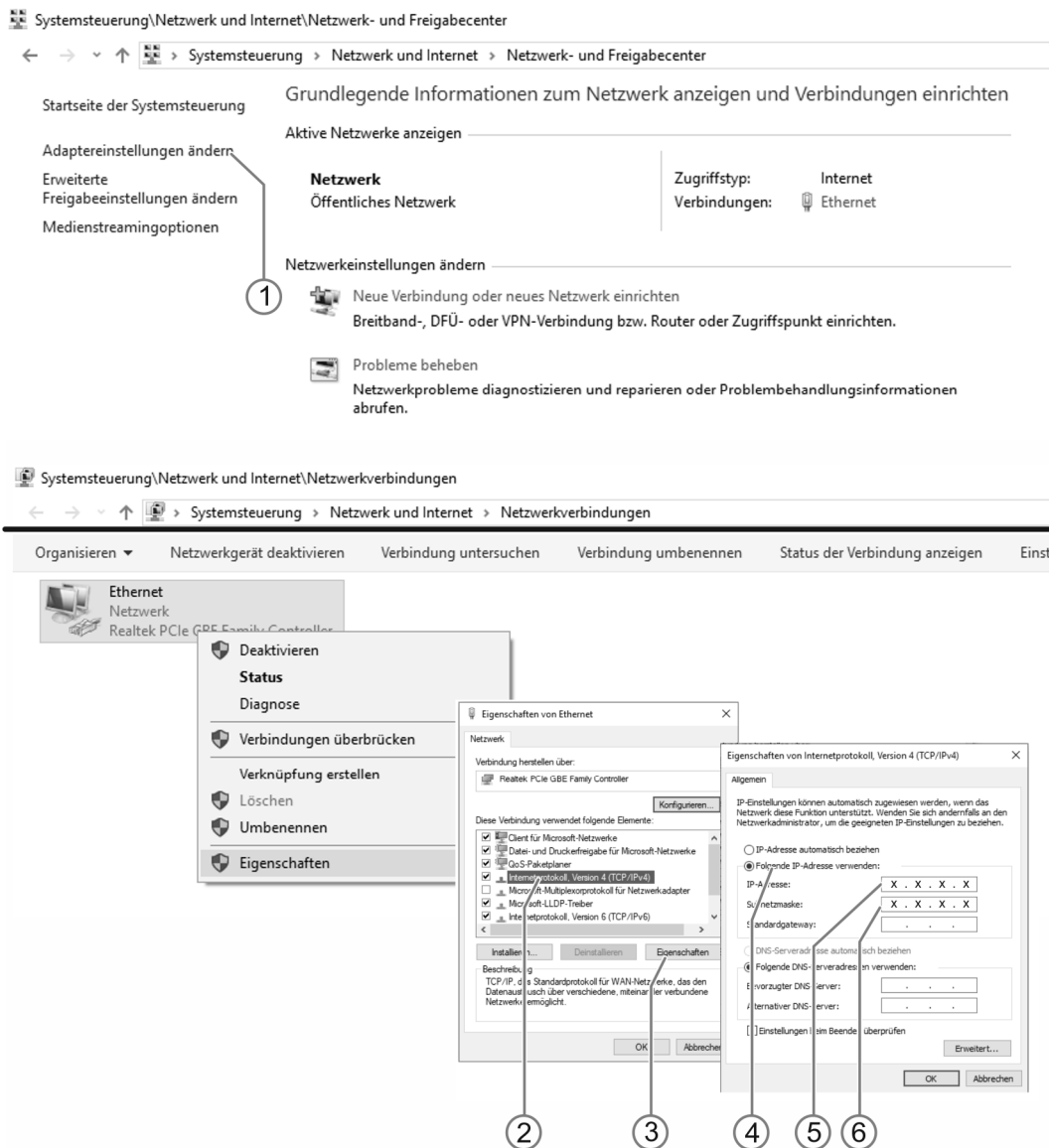


Abb. 34: IP-Adresse im PC einstellen (Beispiel Windows 10)

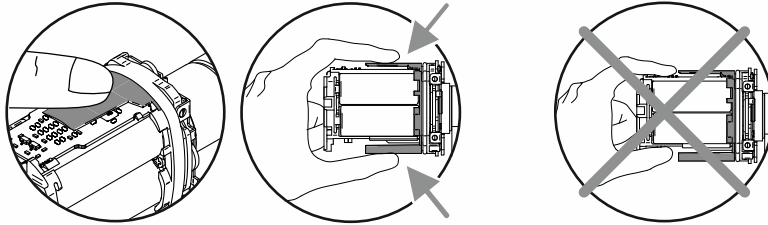
Führen Sie zum Einstellen der IP-Adresse die folgenden Schritte durch:

1. In die Systemsteuerung wechseln.
2. Öffnen: Das Netzwerk- und Freigabecenter.
 - „Netzwerk und Internet“ / „Netzwerk- und Freigabecenter“.
3. Öffnen: „Adaptoreinstellungen ändern“ [1].
 - Das Dialogfeld „Netzwerkverbindungen“ wird angezeigt.
4. Im Dialogfeld die Netzwerkverbindung markieren und mit Rechtsklick öffnen: Eigenschaften [3].
5. Im Dialogfeld markieren: „Internetprotokoll Version 4 (TCP/IPv4)“ [2].
6. Im Dialogfeld öffnen: Eigenschaften [3].
7. Im Dialogfeld aktivieren: Folgende IP-Adresse verwenden [4].
8. Bei „IP-Adresse die gewünschte IP-Adresse eintippen [5].
9. Bei „Subnetzmaske“: Nur hineinklicken [6].
 - Die Adresse wird automatisch gefunden.
10. Bestätigen und alle Fenster schließen.

Das Gerät lässt sich jetzt über einen Webbrowser aufrufen.

3.2 Geräte hinzufügen

3.2.1 „Elektronischer Schließzylinder“



Achtung! – Beschädigung der Elektronik

Beim Berühren der elektronischen Bauteile können diese durch elektrostatische Entladung eines Menschen beschädigt werden.

- Halten Sie nach dem Abziehen des Knaufgehäuses den Leseknauf an dem dafür vorgesehenen Berührungsschutz.

Das Inbetriebnehmen der „Elektronischer Schließzylinder“ erfolgt bei allen Profilarten in derselben Weise.

Für das Inbetriebnehmen der „Elektronischer Schließzylinder“ sind die folgenden Punkte Voraussetzung:

- Eine Verbindung zum „Smart Access Point Pro“. Dies muss der „Smart Access Point Pro“ sein, der in dem System eingesetzt wird.
 - „Smart Access Point Pro“:
 - Der „Smart Access Point Pro“ muss betriebsbereit sein.
 - Ein PC ist mit dem „Smart Access Point Pro“ verbunden.
 - Die Verwaltungssoftware des „Smart Access Point Pro“ ist auf dem PC geöffnet.
- Die Seriennummer des „Elektronischer Schließzylinder“. Diese befindet sich in dem Leseknauf.
- Die Batterien des „Elektronischer Schließzylinder“ (liegen bei).
- Die Installationskarte.
- Sollen mit der Inbetriebnahme bereits Schließberechtigungen für Personen erteilt werden, sind ebenfalls die Transponderschlüssel erforderlich.
 - Vor allem bei größeren Projekten ist es jedoch empfehlenswert, dies gesondert durchzuführen.
 - Für das Erteilen von Schließrechten, siehe Kapitel 5.5 „Benutzerverwaltung“ auf Seite 118.

Führen Sie für das Inbetriebnehmen der „Elektronischer Schließzylinder“ die folgenden Punkte durch:

1. Sicherstellen, dass zwischen dem Lesekopf und dem „Smart Access Point Pro“ eine Funkverbindung besteht. Die Funkverbindung kann dabei über unterschiedliche Wege realisiert werden.
 - Der „Elektronischer Schließzylinder“ ist bereits montiert:
 - Die Kommunikation erfolgt direkt mit dem „Smart Access Point Pro“ oder über die bereits vorhandene Installation von zwischengeschalteten **Zusatzgeräten (Repeater / RF/IP-Gateways)**.
 - Ist die Kommunikation noch nicht möglich, muss der Leseknauf des „Elektronischer Schließzylinder“ demontiert und in die Nähe des „Elektronischer Schließzylinder“ gebracht werden. Weitere Informationen hierzu: siehe Kapitel 3.2.2 „„Elektronischer Schließzylinder“ vorab hinzufügen“ auf Seite 47.
 - Der „Elektronischer Schließzylinder“ ist noch nicht montiert:
 - Der „Elektronischer Schließzylinder“ wird zusammen mit erforderlichen Zusatzgeräten in die Funkreichweite des „Smart Access Point Pro“ gebracht. Weitere Informationen hierzu: siehe Kapitel 3.2.2 „„Elektronischer Schließzylinder“ vorab hinzufügen“ auf Seite 47.

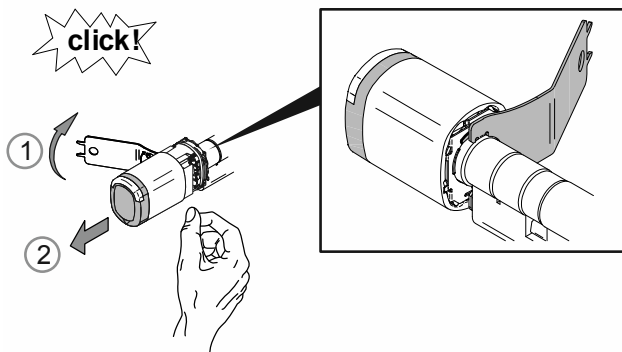


Abb. 35: Knaufgehäuse abziehen

2. Das Knaufgehäuse des Leseknaufs mit dem Montagewerkzeug entriegeln [1] und abziehen [2].

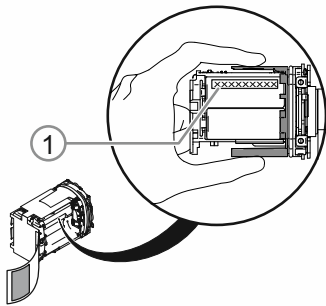


Abb. 36: Seriennummer

3. Die Seriennummer [1] notieren.
 - Die Seriennummer wird zur Anmeldung in der Verwaltungssoftware des „Smart Access Point Pro“ benötigt.
 - Alternativ ist ein Scannen des QR-Codes und Anmelden mit der Busch-Welcome® App möglich.

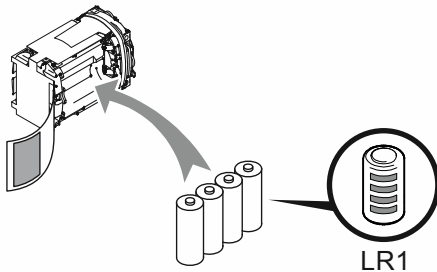


Abb. 37: Batterien einlegen

4. Die Batterien des „Elektronischer Schließzylinder“ einlegen.

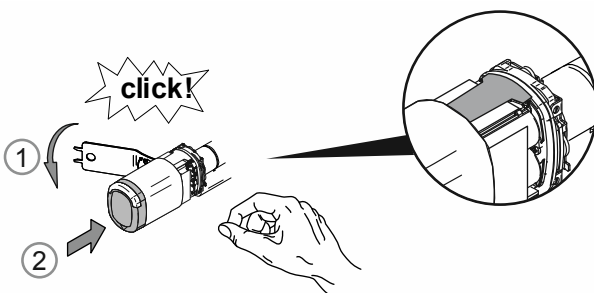


Abb. 38: Knaufgehäuse montieren

5. Das Knaufgehäuse des Leseknaufs wieder montieren.
 - Dabei darauf achten, dass der Berührungsschutz innerhalb des Knaufgehäuses bleibt und beim Montagevorgang nicht geknickt wird.

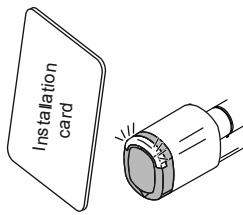


Abb. 39: Installationskarte

6. Den Leseknauf mit der Installationskarte am „Smart Access Point Pro“ anmelden.
 - Für das Anmelden des Leseknaufs in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.
 - Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.2.2 „„Elektronischer Schließzylinder“ hinzufügen“ auf Seite 89.
 - Der Leseknauf ist in der Liste der verfügbaren Geräte hinzugefügt.
7. Den Leseknauf in der Gebäudestruktur des „Smart Access Point Pro“ platzieren.
 - Für das Platzieren des Leseknaufs in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.
 - Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.4.3 „„Elektronischer Schließzylinder“ platzieren“ auf Seite 110.
 - Ist die Gebäudestruktur noch nicht vorhanden, diese zunächst erstellen, siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95.
8. Den Leseknauf in der Gebäudestruktur des „Smart Access Point Pro“ mit dem „Smart Access Point Pro“, „RF/IP Gateway“ oder einem „RF Repeater“ koppeln.
 - Für das Koppeln des Leseknaufs in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.
 - Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.4.4 „Elektronischer Schließzylinder mit Smart Access Point koppeln“ auf Seite 112.
 - Ist der „Smart Access Point Pro“, „RF/IP Gateway“ oder „RF Repeater“ noch nicht platziert, dies zunächst durchführen, siehe Kapitel 5.2 „Gerätekonfiguration“ auf Seite 87 und siehe Kapitel 5.4 „Zutrittskontrolle“ auf Seite 103.

Ist der „Elektronischer Schließzylinder“ in der Verwaltungssoftware des „Smart Access Point Pro“ angemeldet, platziert und gekoppelt, lassen sich für das Schloss Schließrechte für Personen erstellen.

- Für das Erteilen von Schließrechten in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.
- Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.5 „Benutzerverwaltung“ auf Seite 118.

3.2.2 „Elektronischer Schließzylinder“ vorab hinzufügen

Das Hinzufügen der „Elektronischer Schließzylinder“ kann vor allem bei größeren Projekten eine zeitraubende und umständliche Angelegenheit werden. Insbesondere, wenn die „Elektronischer Schließzylinder“ weiter entfernt vom „Smart Access Point Pro“ montiert sind.

In solchen Fällen ist es empfehlenswert, alle Geräte („Elektronischer Schließzylinder“, Repeater, etc.) vor der Montage direkt am „Smart Access Point Pro“ in Betrieb zu nehmen und erst später an ihren Einsatzort zu montieren. Erstellen Sie sich dafür einen entsprechenden Plan.

Bei dieser Vorgehensweise gibt es einen Punkt zu beachten. Bei der Inbetriebnahme der „Elektronischer Schließzylinder“ wird der gesamte Kommunikationsweg zwischen dem Leseknauf und dem „Smart Access Point Pro“ in der Verwaltungssoftware hinterlegt. Wird der „Elektronischer Schließzylinder“ mit den evtl. benötigten weiteren Geräten später an den Einsatzort montiert, muss dieser Kommunikationsweg übereinstimmen. Tut er das nicht, wird der jeweilige „Elektronischer Schließzylinder“ als nicht erkannt angezeigt und muss neu in Betrieb genommen werden.

Dies gilt ebenfalls, sollte ein „Elektronischer Schließzylinder“ zu einem späteren Zeitpunkt einmal an einem anderen Einsatzort montiert werden.



Hinweis

Diese etwas komplexe Inbetriebnahme erfolgt vor dem Hintergrund, dass die gesamte Gerätesteuerung außerhalb der batteriebetriebenen Zuganggeräte erfolgt. Dadurch wird der Energieverbrauch der Leseköpfe minimiert und die Batterielebensdauer entsprechend erhöht.

3.2.3 „RF/IP Gateway“

Für das Inbetriebnehmen des „RF/IP Gateway“ sind die folgenden Punkte Voraussetzung:

- Der „RF/IP Gateway“ ist im Netzwerk angeschlossen.
- Die Spannungsversorgung des „RF/IP Gateway“ ist hergestellt.
 - Über PoE oder über eine gesonderte 24 V Spannungsversorgung.
- Die Seriennummer des „RF/IP Gateway“. Diese befindet sich auf dem Gerät.
- Der „Smart Access Point Pro“ ist betriebsbereit. Dies muss der „Smart Access Point Pro“ sein, der in dem System eingesetzt wird.
 - „Smart Access Point Pro“:
 - Ein PC ist mit dem „Smart Access Point Pro“ verbunden.
 - Die Verwaltungssoftware des „Smart Access Point Pro“ ist auf dem PC geöffnet.

Ist die Inbetriebnahme vorbereitet, wird der „RF/IP Gateway“ in der Verwaltungssoftware des „Smart Access Point Pro“ hinzugefügt.

Führen Sie für das Inbetriebnehmen des „RF/IP Gateway“ die folgenden Punkte durch:

1. Den „RF/IP Gateway“ im „Smart Access Point Pro“ hinzufügen.
 - Für das Hinzufügen in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.
 - Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.2.3 „„RF/IP Gateway“ hinzufügen“ auf Seite 91.
2. Den „RF/IP Gateway“ in der Gebäudestruktur des „Smart Access Point Pro“ platzieren.
 - Für das Platzieren des „RF/IP Gateway“ in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.

- Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.4.2 „RF/IP Gateway“ platzieren“ auf Seite 107.
- Ist die Gebäudestruktur noch nicht vorhanden, diese zunächst erstellen, siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95.



Hinweis

Je nach der Installation kann es sehr sinnvoll sein, den „RF/IP Gateway“ vorab zusammen mit den „Elektronischer Schließzylinder“ in Betrieb zu nehmen.

- Für eine Vorabinbetriebnahme, siehe Kapitel 3.2.2 „Elektronischer Schließzylinder“ vorab hinzufügen“ auf Seite 47.

3.2.4 Repeater

Für das Inbetriebnehmen des „RF Repeater“ sind die folgenden Punkte Voraussetzung:

- Die Spannungsversorgung des „RF Repeater“ ist hergestellt.
 - Die Spannungsversorgung erfolgt über eine gesonderte 24 V Spannungsversorgung.
- Die Seriennummer des „RF Repeater“. Diese befindet sich auf dem Gerät.
- Eine Verbindung zum „Smart Access Point Pro“. Dies muss der „Smart Access Point Pro“ sein, der in dem System eingesetzt wird.
 - „Smart Access Point Pro“:
 - Der „Smart Access Point Pro“ muss betriebsbereit sein.
 - Ein PC ist mit dem „Smart Access Point Pro“ verbunden.
 - Die Verwaltungssoftware des „Smart Access Point Pro“ ist auf dem PC geöffnet.

Führen Sie für das Inbetriebnehmen des „RF Repeater“ die folgenden Punkte durch:

1. Sicherstellen, dass zwischen dem „RF Repeater“ und dem „Smart Access Point Pro“ eine Funkverbindung besteht. Die Funkverbindung kann dabei über unterschiedliche Wege realisiert werden.
 - Der „RF Repeater“ ist bereits montiert:
 - Die Kommunikation erfolgt direkt mit dem „Smart Access Point Pro“ oder über die bereits vorhandene Installation von zwischengeschalteten weiteren „RF Repeater“.
 - Ist die Kommunikation noch nicht möglich, muss der „RF Repeater“ demontiert und in die Nähe des „Elektronischer Schließzylinder“ gebracht werden. Weitere Informationen hierzu: siehe Kapitel 3.2.2 „Elektronischer Schließzylinder“ vorab hinzufügen“ auf Seite 47.
 - Der „RF Repeater“ ist noch nicht montiert:
 - Der „RF Repeater“ wird zusammen mit erforderlichen Zusatzgeräten in die Funkreichweite des „Smart Access Point Pro“ gebracht. Weitere Informationen hierzu: siehe Kapitel 3.2.2 „Elektronischer Schließzylinder“ vorab hinzufügen“ auf Seite 47.
2. Den „RF Repeater“ im „Smart Access Point Pro“ hinzufügen.
 - Für das Hinzufügen in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.
 - Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.2.4 „RF Repeater“ hinzufügen“ auf Seite 93.
3. Den „RF Repeater“ in der Gebäudestruktur des „Smart Access Point Pro“ platzieren.
 - Für das Platzieren des „RF Repeater“ in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.

- Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.4.5 „Repeater platzieren“ auf Seite 115.
 - Ist die Gebäudestruktur noch nicht vorhanden, diese zunächst erstellen, siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95.
- 4. Den „RF Repeater“ in der Gebäudestruktur des „Smart Access Point Pro“ mit dem „Smart Access Point Pro“, „RF/IP Gateway“ oder einem weiteren „RF Repeater“ koppeln.
 - Für das Koppeln in die Verwaltungssoftware des „Smart Access Point Pro“ wechseln.
 - Für die erforderlichen Schritte in der Verwaltungssoftware, siehe Kapitel 5.4.6 „Repeater koppeln“ auf Seite 116.
 - Ist der „Smart Access Point Pro“, „RF/IP Gateway“ oder ein weiterer „RF Repeater“ noch nicht platziert, dies zunächst durchführen, siehe Kapitel 5.2 „Gerätekonfiguration“ auf Seite 87 und siehe Kapitel 5.4 „Zutrittskontrolle“ auf Seite 103.



Hinweis

Je nach der Installation kann es sehr sinnvoll sein, den „RF Repeater“ vorab zusammen mit den „Elektronischer Schließzylinder“ in Betrieb zu nehmen.

- Für eine Vorabinbetriebnahme, siehe Kapitel 5.5 „Benutzerverwaltung“ auf Seite 118.

3.3 Gerät löschen im „Smart Access Point“

3.3.1 „Elektronischer Schließzylinder“

Soll der „Elektronischer Schließzylinder“ aus dem System entfernt werden, wird dies in der Verwaltungssoftware des „Smart Access Point Pro“ durchgeführt.

- Für die erforderlichen Schritte in der Verwaltungssoftware:
 - siehe Kapitel 5.7.1 „Elektronischer Schließzylinder von Smart Access Point Pro entkoppeln“ auf Seite 135.
 - siehe Kapitel 5.7.2 „Elektronischer Schließzylinder aus dem Raum entfernen“ auf Seite 138.
 - siehe Kapitel 5.8.1 „Elektronischer Schließzylinder aus dem System löschen“ auf Seite 144.

3.3.2 „RF/IP Gateway“

Soll der „RF/IP Gateway“ aus dem System entfernt werden, wird dies in der Verwaltungssoftware des „Smart Access Point Pro“ durchgeführt.

- Für die erforderlichen Schritte in der Verwaltungssoftware:
 - .
 - .

3.3.3 Repeater

Soll der „RF Repeater“ aus dem System entfernt werden, wird dies in der Verwaltungssoftware des „Smart Access Point Pro“ durchgeführt.

- Für die erforderlichen Schritte in der Verwaltungssoftware:
 - siehe Kapitel 5.7.4 „Repeater entkoppeln“ auf Seite 140.
 - siehe Kapitel 5.7.5 „Repeater aus dem Raum entfernen“ auf Seite 142.
 - siehe Kapitel 5.8.3 „Repeater aus dem System löschen“ auf Seite 146.

3.4 Projekt sichern / Wiederherstellen (Backup / Restore)

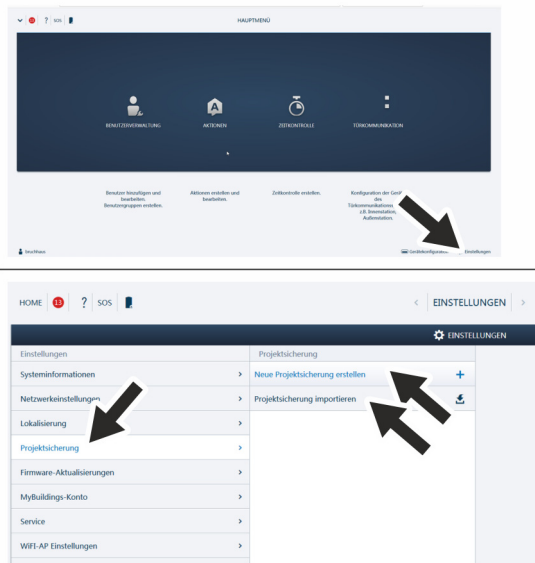


Abb. 40: Datensicherung / Datenwiederherstellung

Erstellen Sie nach Abschluss der ersten Initialisierung eine erste Datensicherung.

Erstellen Sie danach bei jeder größeren Änderung, wie z.B. dem Hinzufügen oder Löschen von Geräten, eine Datensicherung.

Führen Sie zum Erstellen der Datensicherung die folgenden Punkte durch:

1. Einen PC mit dem „Smart Access Point“ verbinden.
 - Nähere Informationen zum Verbinden, siehe Kapitel 3.1.2 „Einen PC mit dem „Smart Access Point“ Verbinden“ auf Seite 30.
2. Im Hauptmenü des „Smart Access Point“ in die Funktion „Einstellungen“ wechseln.
3. In die Funktion „Projektsicherung“ wechseln.

Datensicherung erstellen

1. Über die Funktion „Neue Projektsicherung erstellen“ wird die Backup-Datei erstellt.

Datensicherung zurückspielen

1. Über die Funktion „Projektsicherung importieren“ wird die Backup-Datei importiert.

Datenverlust



Hinweis

Existiert kein Backup und die Daten im „Smart Access Point“ gehen verloren, können die batteriegetriebenen Zugangssysteme für eine Neuinbetriebnahme nicht mehr entkoppelt werden. Die alten Daten verbleiben in den Leseköpfen. Da es sich um Schließsysteme handelt, ist ein Zugriff von außen nicht möglich. Es könnte sich um einen unbefugten Zugriff handeln.

- Die batteriegetriebenen Zugangssysteme müssen dann im Herstellerwerk zurückgesetzt werden.
- Achten sie also unbedingt darauf, ein Backup der Daten des „Smart Access Point“ zu besitzen.

3.5 RESET (System / Geräte zurücksetzen)

3.5.1 „Smart Access Point“

Den „Smart Access Point“ komplett zurücksetzen.

- Hierbei werden sämtliche eingegebenen Daten, durchgeführte Einstellungen, etc. gelöscht. Der „Smart Access Point“ befindet sich nach dem Zurücksetzen im Auslieferungszustand.
- Nach dem Zurücksetzen muss eine Erstinbetriebnahme des „Smart Access Point“ durchgeführt werden.
- Nach der neuen Erstinbetriebnahme können ältere Daten über ein vorhandenes Backup wieder eingespielt werden.

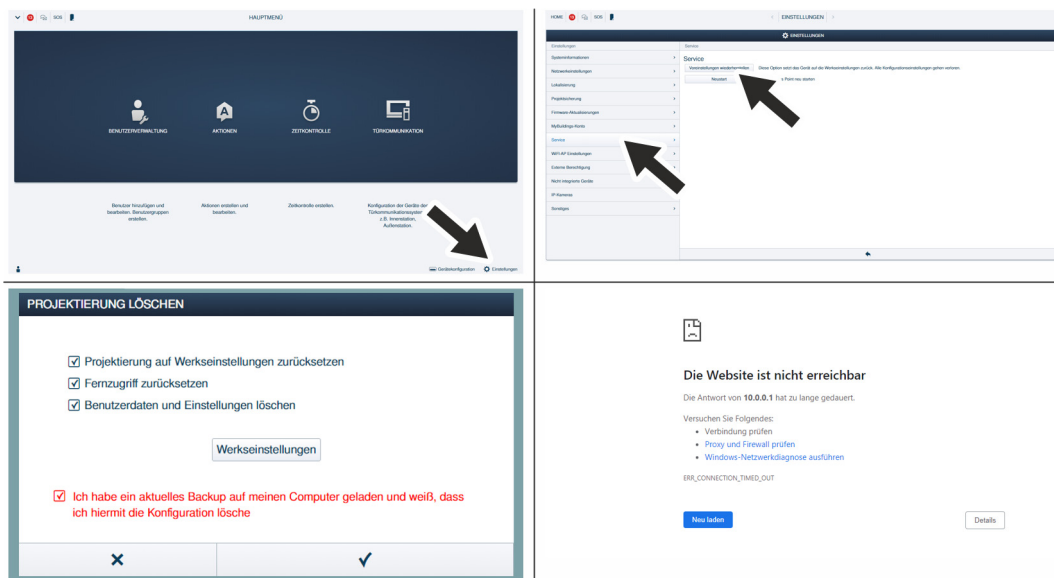


Abb. 41: „Smart Access Point“ komplett zurücksetzen

Führen Sie zum Zurücksetzen die folgenden Schritte durch:

1. Einen PC mit dem „Smart Access Point“ verbinden.
 - Nähere Informationen zum Verbinden, siehe Kapitel 3.1.2 „Einen PC mit dem „Smart Access Point“ Verbinden“ auf Seite 30.
2. In die Funktion „Einstellungen“ / „Service“ wechseln.
3. Die Funktion „Voreinstellungen wiederherstellen“ aufrufen.
4. Die Bereiche auswählen, die zurückgesetzt werden sollen.
5. Die Auswahl bestätigen.
 - Der „Smart Access Point“ wird zurückgesetzt.
 - Nach dem Zurücksetzen ist die Verbindung zum „Smart Access Point“ nicht mehr aktiv.
 - Der „Smart Access Point“ muss über eine Erstinbetriebnahme neu in Betrieb genommen werden, siehe Kapitel 3.1 „Inbetriebnahme des Systems — „Smart Access Point Pro““ auf Seite 30.

4 Planungs- / Anwendungsinformationen

4.1 Funktionsprinzipien / Arbeitsweisen

„Elektronischer Schließzylinder“ mit Transponderschlüssel (Funk-Kommunikationsgerät)

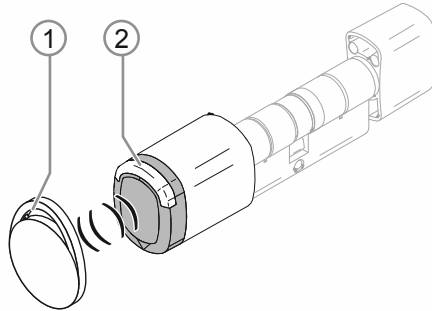


Abb. 42: „Elektronischer Schließzylinder“ mit Transponderschlüssel

- [1] Transponderschlüssel in Form eines Anhängers
- [2] Leseknauf „Elektronischer Schließzylinder“

Der „Elektronischer Schließzylinder“ wird mithilfe eines Transponderschlüssels über RFID geschaltet. Bei dem RFID-Transponderschlüssel handelt es sich um einen kleinen Anhänger, der einen programmierten Chip enthält. Durch den Transponderschlüssel, der vor den Leseknauf des „Elektronischer Schließzylinder“ gehalten wird, erhalten Zutrittsberechtigte Zutritt zum Gebäude oder Raum.

Jeder Transponderschlüssel besitzt seine individuelle Seriennummer, die im „Smart Access Point Pro“ hinterlegt wird. Nur wenn diese Seriennummer als korrekt erkannt wird und der Besitzer ein Schließrecht besitzt, schaltet der Leseknauf und das Schloss lässt sich öffnen.

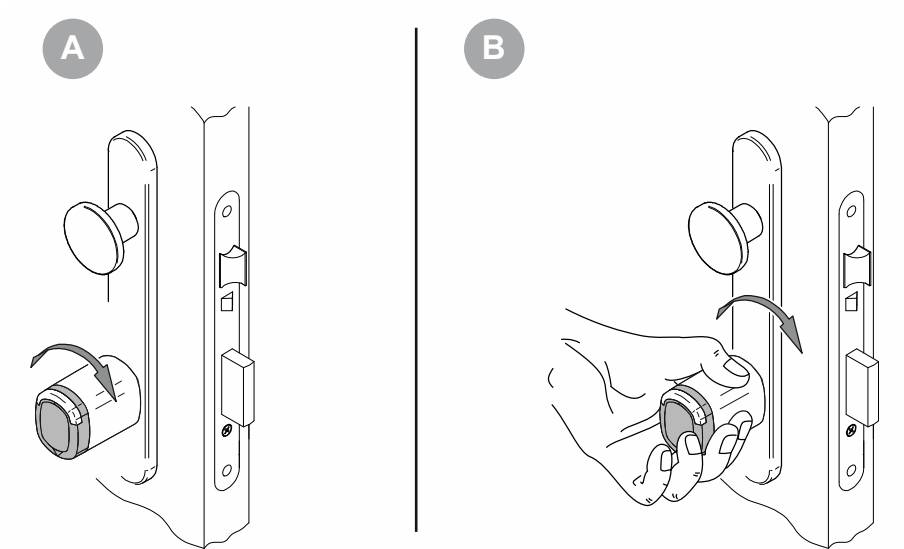
Schaltvorgang des Leseknaufs

Abb. 43: Schaltvorgang des Leseknaufs

Im verriegelten Zustand der Tür lässt sich der Leseknauf frei vor dem Schließzylinder drehen (A). Es ist keine Bedienung des Schließzylinders möglich. Erst wenn ein Zutrittsberechtigter seinen Transponderschlüssel vor den Leseknauf hält, schaltet der Leseknauf und stellt für einige Sekunden eine mechanische Verbindung zum Schließzylinder her. Das Schloss lässt sich öffnen (B). Nach Ablauf der voreingestellten Zeit schaltet der Leseknauf wieder automatisch in den verriegelten Zustand der Tür.

Kommunikation des Leseknaufs

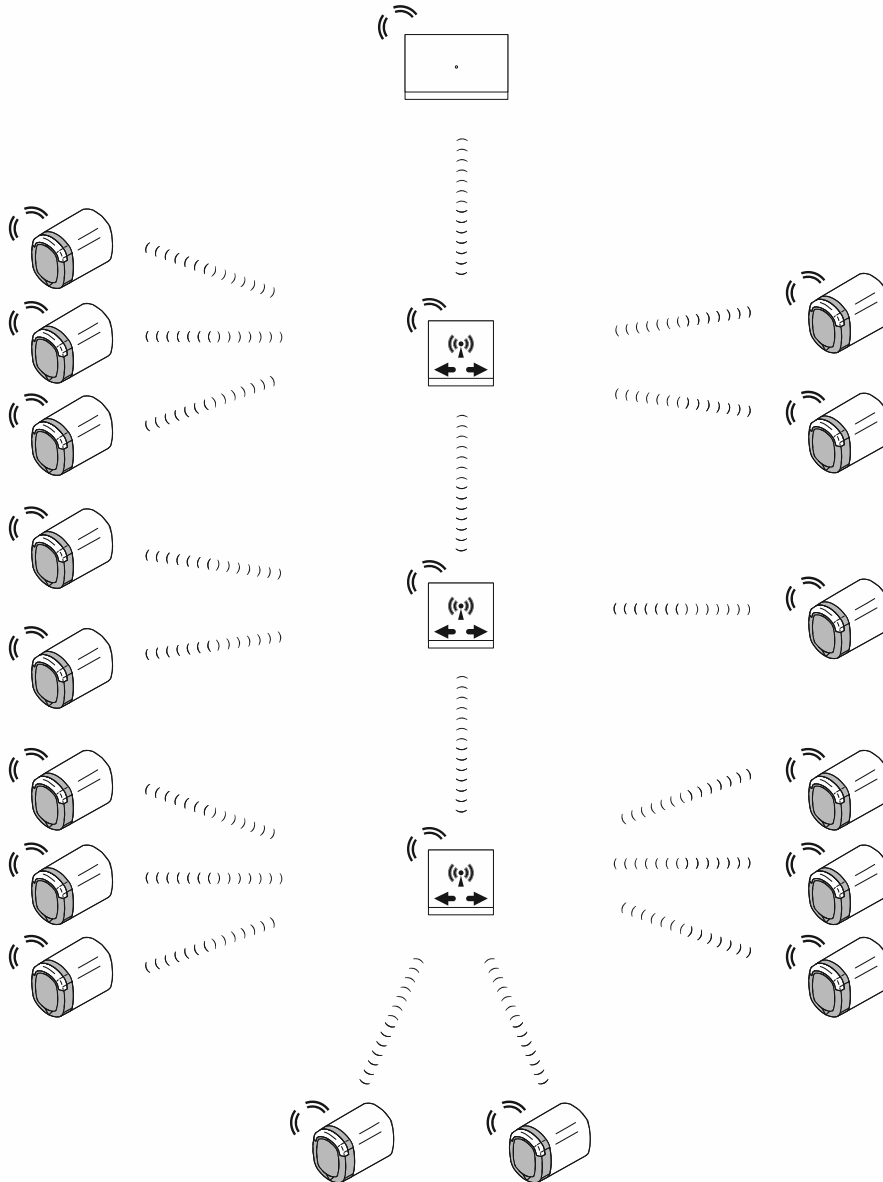


Abb. 44: Kommunikation des Leseknaufs

Die Kommunikation des Leseknaufs mit der Verwaltungssoftware des „Smart Access Point Pro“ erfolgt über die Funkfrequenzen des Bluetooth. Die Reichweite zwischen den einzelnen Geräten beträgt dadurch etwa 10 Meter.

- Für die Erhöhung der Reichweite werden Repeater eingesetzt. Mit dem Einsatz von Repeatern lässt sich die Gesamtreichweite in einer Funklinie auf etwa 40 Meter erhöhen.
- Wird eine größere Reichweite als 40 Meter benötigt, wird dies über den zusätzlichen Einsatz von RF/IP Gateways realisiert.



Hinweis

Es werden nur die Frequenzen des Bluetooth verwendet. Die gängigen Funktionalitäten des Bluetooth sind nicht integriert (z.B. Sichtbarkeit des Lesekopfes auf einem Smartphone).

4.2 Kapazität / Reichweite

Übersicht

Systemkapazität „Busch-AccessControl“	
Verwaltungssoftware im „Smart Access Point Pro“	Bis zu 600 Geräte

Tab.6: Systemkapazität „Busch-AccessControl“

Ansteuerungskapazität	
„Smart Access Point Pro“	Bis zu 16 „Elektronischer Schließzylinder“ Bis zu 3 Repeater Bis zu 64 RF/IP Gateway
Repeater	Bis zu 16 „Elektronischer Schließzylinder“ – Durchschleifen der Kapazität des „Smart Access Point Pro“ / RF/IP Repeaters
RF/IP Gateway	Bis zu 16 „Elektronischer Schließzylinder“ Bis zu 3 Repeater

Tab.7: Ansteuerungskapazität

Reichweiten	
Funkreichweite zwischen 2 einzelnen Geräten	Ca. 10 Meter
Funkreichweite innerhalb einer Funklinie	Ca. 40 Meter
Systemreichweite über Funk und IP-Netzwerk	Bis ca. 1,5 Kilometer

Tab.8: Reichweiten

Funkreichweite

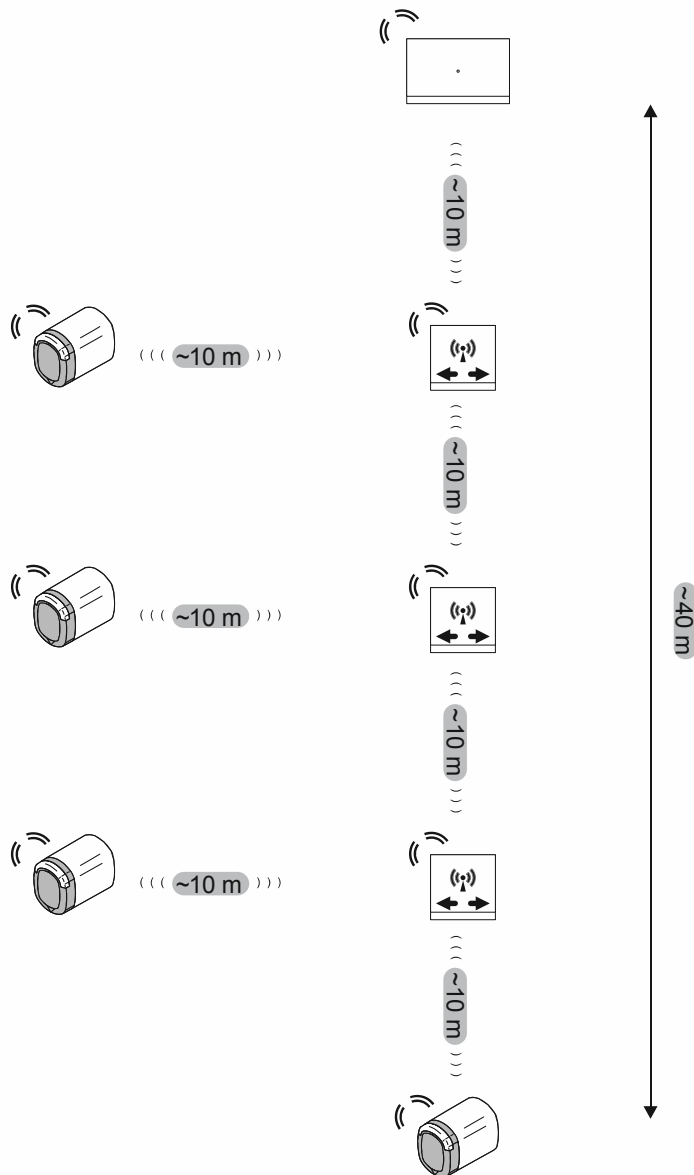


Abb. 45: Funkreichweite zwischen Geräten

Die Funkreichweite beträgt zwischen jedem Gerät maximal etwa 10 Meter.

Von einem „Smart Access Point Pro“ oder RF/IP Gateway aus gesehen lassen sich bis zu 3 Repeater hintereinanderschalten. Solch eine Reihe bildet eine Funklinie.

Daraus ergibt sich eine maximale Funkreichweite zwischen einem „Smart Access Point Pro“ oder RF/IP Gateway bis zum entferntesten „Elektronischer Schließzylinder“ von etwa 40 Metern.

Maximale Anzahl von Schließzylindern in einer Funklinie

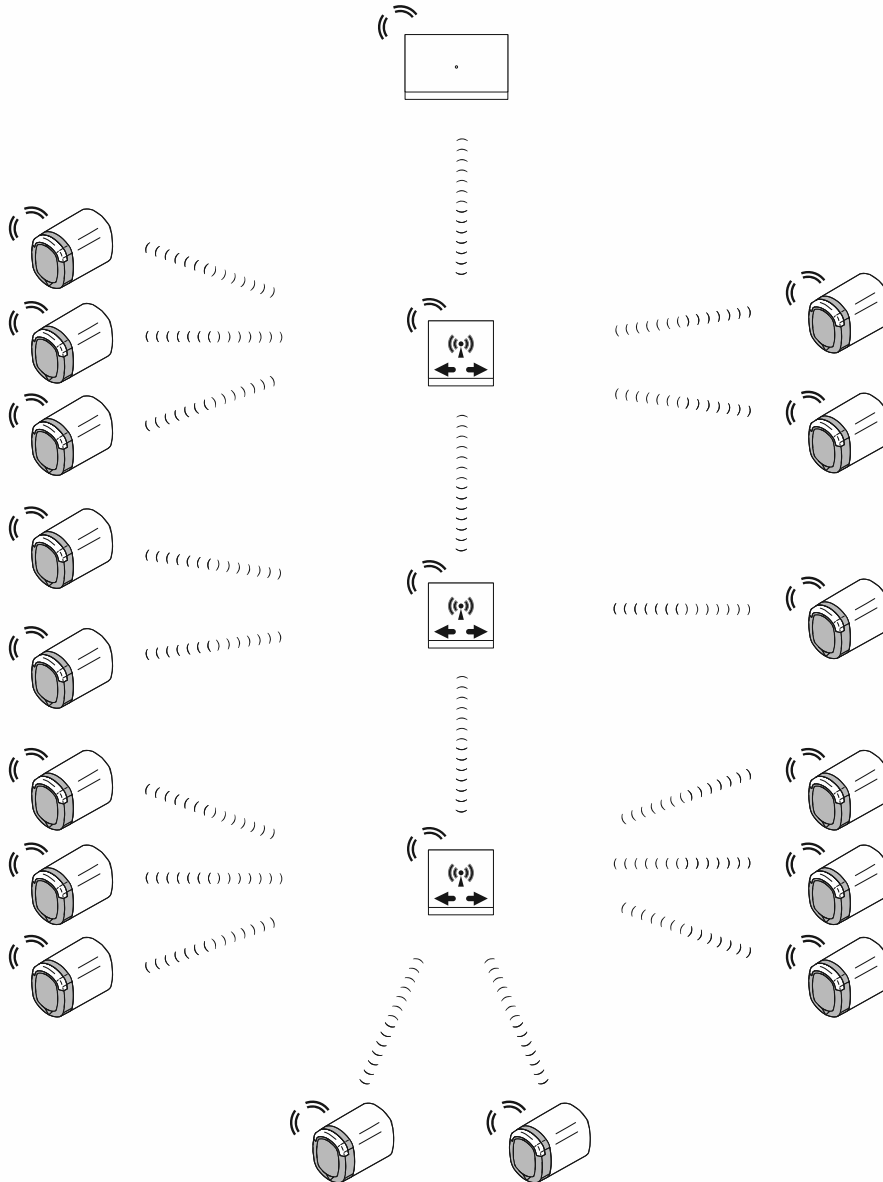


Abb. 46: Maximale Anzahl von Schließzylindern in einer Funklinie

In einer Funklinie lassen sich insgesamt bis zu 16 „Elektronischer Schließzylinder“ über den „Smart Access Point Pro“ oder einem RF/IP Gateway ansteuern.

Die „Elektronischer Schließzylinder“ lassen sich in der Funklinie an den Repeatern frei verteilen. Jeder Repeater in der Funklinie kann von 0 bis 16 „Elektronischer Schließzylinder“ bedienen.

- Insgesamt darf dabei die maximale Anzahl von 16 „Elektronischer Schließzylinder“ in der Funklinie nicht überschritten werden.

An dem „Smart Access Point Pro“ oder RF/IP Gateway selbst lassen sich keine „Elektronischer Schließzylinder“ bedienen, wenn die Signale an Repeater weitergeleitet werden.

Gesamtkapazität und Gesamtreichweite

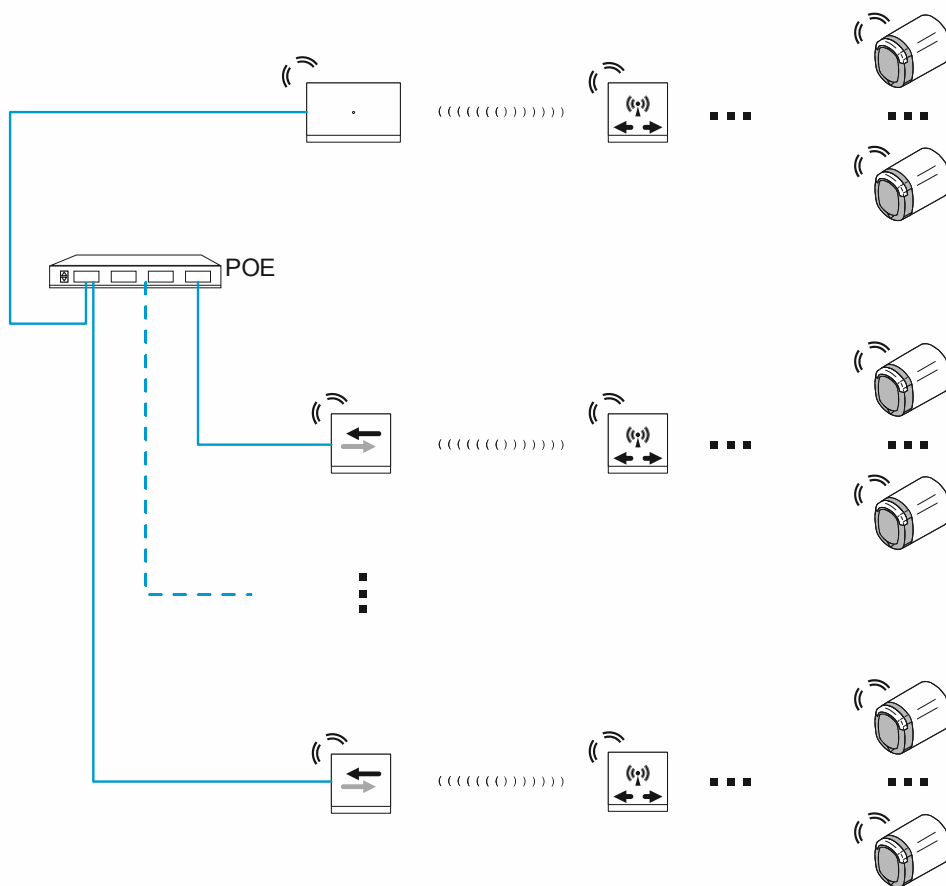


Abb. 47: Gesamtkapazität und Gesamtreichweite

Von einem „Smart Access Point Pro“ aus lassen sich bis zu 64 RF/IP Gateways ansteuern. Von diesen aus lassen sich zusätzlich zum „Smart Access Point Pro“ jeweils in einer eigenen Funklinie bis zu 16 „Elektronischer Schließzylinder“ ansteuern. Dies ergibt eine theoretische Gesamtkapazität von 1040 „Elektronischer Schließzylinder“ in einem System. Die Kapazität der Verwaltungssoftware ist jedoch auf 600 Geräte begrenzt. Die Gesamtanzahl aller Geräte („Elektronischer Schließzylinder“, Repeater, etc.) in einem System darf daher 600 nicht überschreiten.

Die maximale Reichweite in einer einzelnen Funklinie von etwa 40 Metern reicht oft nicht aus. In diesem Fall werden die entfernter liegenden Geräte über RF/IP Gateways mit eigenen Funklinien angesteuert. Die realisierbare Reichweite innerhalb eines Systems „Busch-AccessControl“ wird damit nur über die Reichweite des IP-Netzwerkes begrenzt.

- Zu den Einzelheiten der realisierbaren Reichweiten innerhalb eines IP-Netzwerkes siehe Kapitel 1.5 „Grundlagen strukturierter Verkabelung“ auf Seite 9.

**Hinweis**

- Liegen innerhalb einer geplanten Funklinie dicke Wände, sind die erzielbaren Reichweiten stark herabgesetzt. In diesem Fall ist ein Auftrennen der Funklinie über mehrere RF/IP Gateways sinnvoll.
- Dasselbe gilt für Verbindungen in andere Etagen, wo die Funksignale durch die Etagendecken hindurch müssen. Hier ist es sinnvoll, grundsätzlich für jede Etage eigene RF/IP Gateways einzuplanen.

4.3 Anwendungsbeispiele

4.3.1 Einfamilienhaus

In einer Anlage „Busch-AccessControl“ wird in einem Einfamilienhaus der Haupteingang mit einem „Elektronischer Schließzylinder“ ausgestattet.

Neben dem „Elektronischer Schließzylinder“ ist für die Benutzerverwaltung ein „Smart Access Point Pro“ erforderlich.

- Die Anlage „Busch-AccessControl“ ist in diesem Beispiel nicht mit anderen Systemen vernetzt. Der Einsatz eines PoE-Switch ist nicht vorgesehen, daher benötigt der „Smart Access Point Pro“ eine gesonderte 24 V Spannungsversorgung.

Die Entfernungen liegen innerhalb der Funkreichweite von etwa 10 Metern. Weitere Geräte zur Erhöhung der Reichweiten sind daher nicht notwendig.

Über einen „Smart Access Point Pro“ lassen sich bis zu 16 „Elektronischer Schließzylinder“ ansteuern. Ist die Gesamtzahl der „Elektronischer Schließzylinder“ kleiner, sind weitere Geräte zur Erhöhung der Kapazität nicht notwendig.

Nähere Informationen über die Kapazitäts- und Vernetzungsplanung finden Sie unter: siehe Kapitel 4.2 „Kapazität / Reichweite“ auf Seite 57.

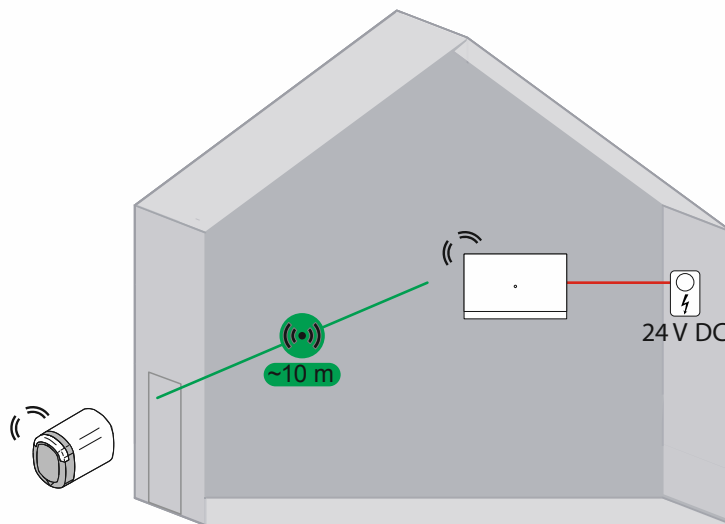


Abb. 48: Übersicht: Einfamilienhaus mit einem „Elektronischer Schließzylinder“

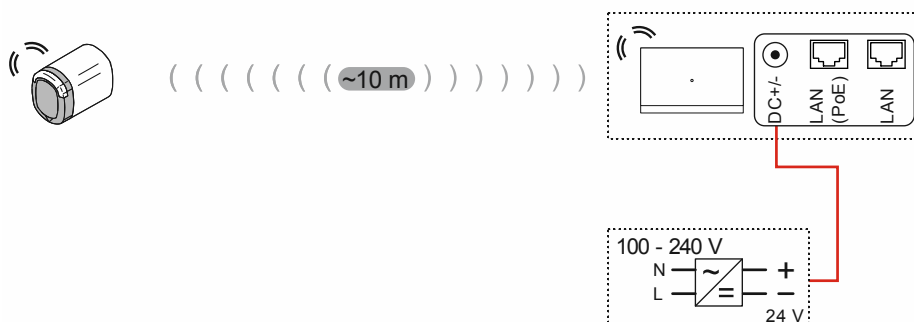


Abb. 49: Anschluss: Einfamilienhaus mit einem „Elektronischer Schließzylinder“

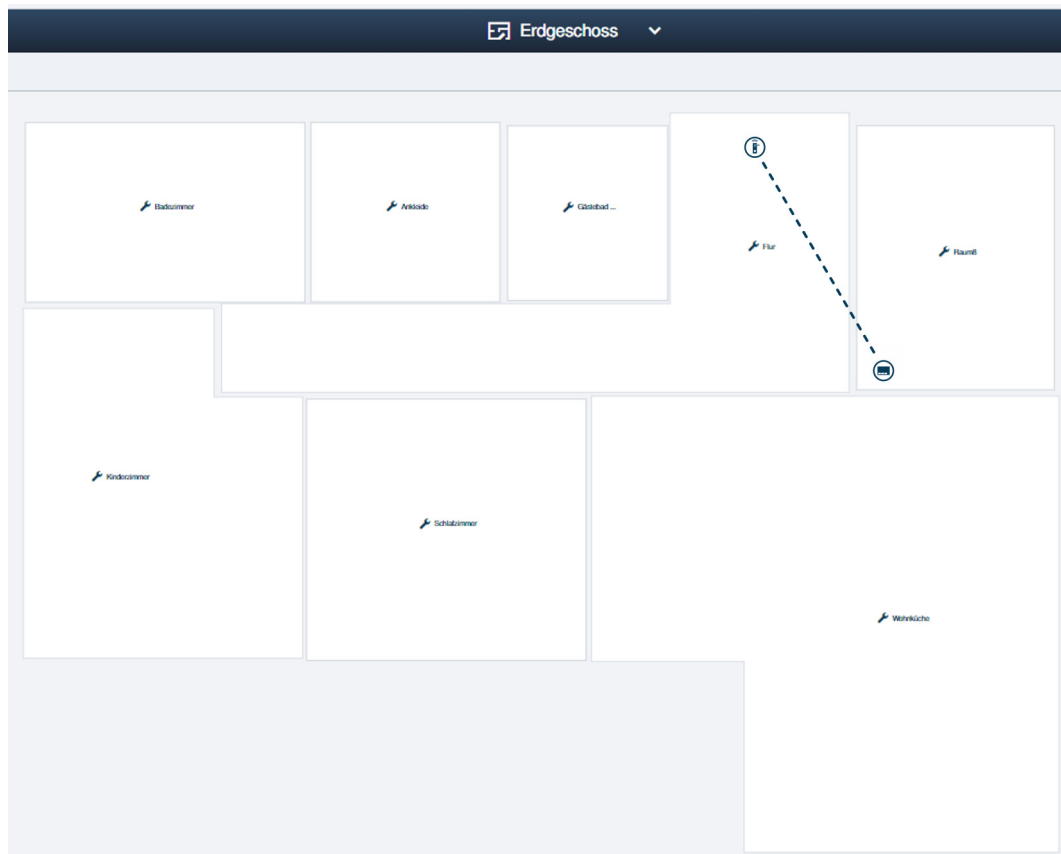


Abb. 50: Gebäudestruktur: Einfamilienhaus mit einem „Elektronischer Schließzylinder“

Beispielaufbau des Erdgeschosses eines Einfamilienhauses in der Verwaltungssoftware des „Smart Access Point Pro“. Der „Elektronischer Schließzylinder“ ist mit dem „Smart Access Point Pro“ verbunden.

- Informationen für die Erstellung einer Gebäudestruktur: siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95

4.3.2 Mehrfamilienhaus mit einem Geschoss

In einer Anlage „Busch-AccessControl“ werden in einem Mehrfamilienhaus der Haupteingang sowie die Wohnungseingänge mit „Elektronischer Schließzylinder“ ausgestattet.

Neben dem „Elektronischer Schließzylinder“ ist für die Benutzerverwaltung ein „Smart Access Point Pro“ erforderlich.

- Die Anlage „Busch-AccessControl“ ist in diesem Beispiel nicht mit anderen Systemen vernetzt. Der Einsatz eines PoE-Switch ist nicht vorgesehen, daher benötigt der „Smart Access Point Pro“ eine gesonderte 24 V Spannungsversorgung.

Die Entfernungen liegen innerhalb der Funkreichweite von etwa 10 Metern. Weitere Geräte zur Erhöhung der Reichweiten sind daher nicht notwendig.

Über einen „Smart Access Point Pro“ lassen sich bis zu 16 „Elektronischer Schließzylinder“ ansteuern. Ist die Gesamtzahl der „Elektronischer Schließzylinder“ kleiner, sind weitere Geräte zur Erhöhung der Kapazität nicht notwendig.

Nähere Informationen über die Kapazitäts- und Vernetzungsplanung finden Sie unter: siehe Kapitel 4.2 „Kapazität / Reichweite“ auf Seite 57.

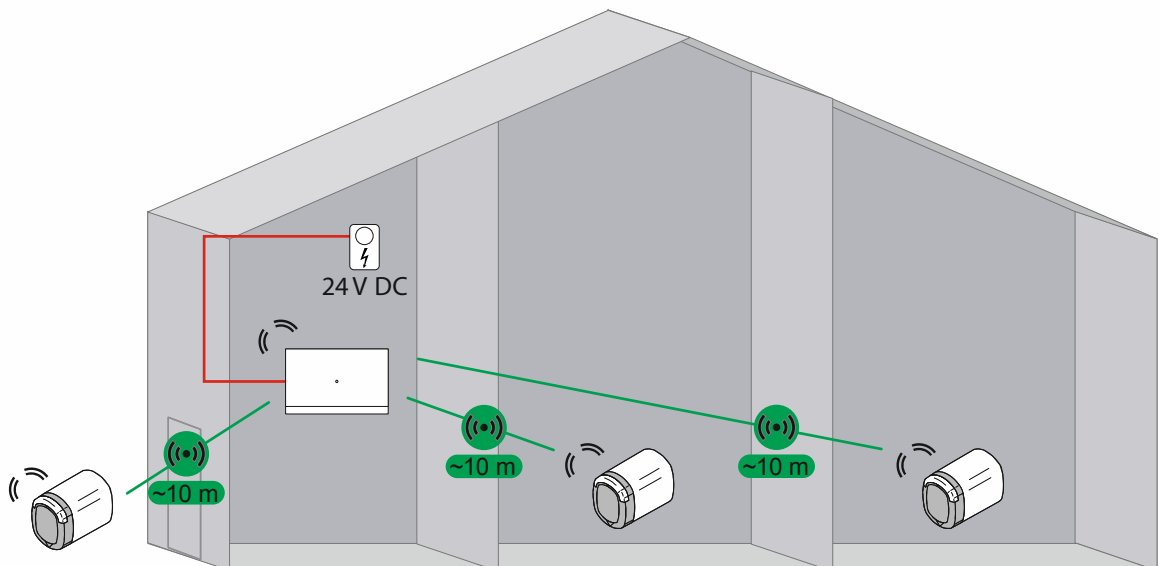


Abb. 51: Übersicht: Mehrfamilienhaus mit 3 „Elektronischer Schließzylinder“

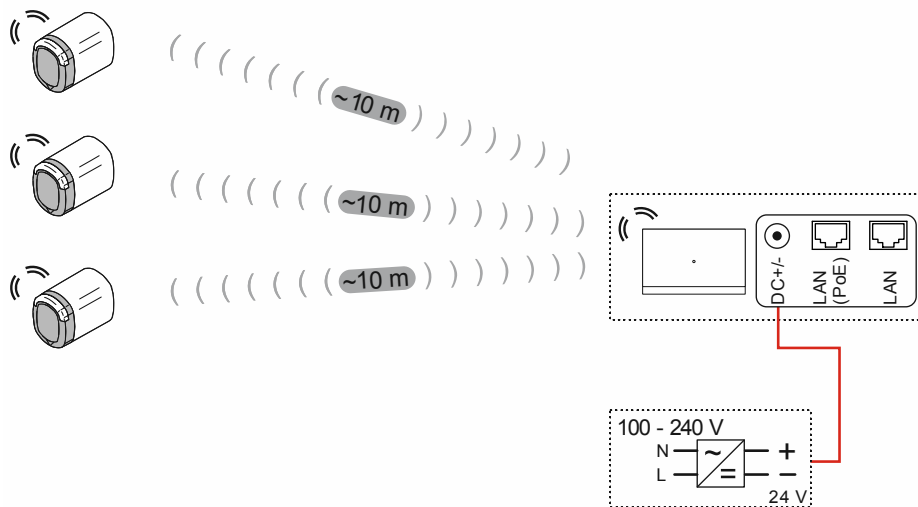


Abb. 52: Anschluss: Mehrfamilienhaus mit 3 „Elektronischer Schließzylinder“

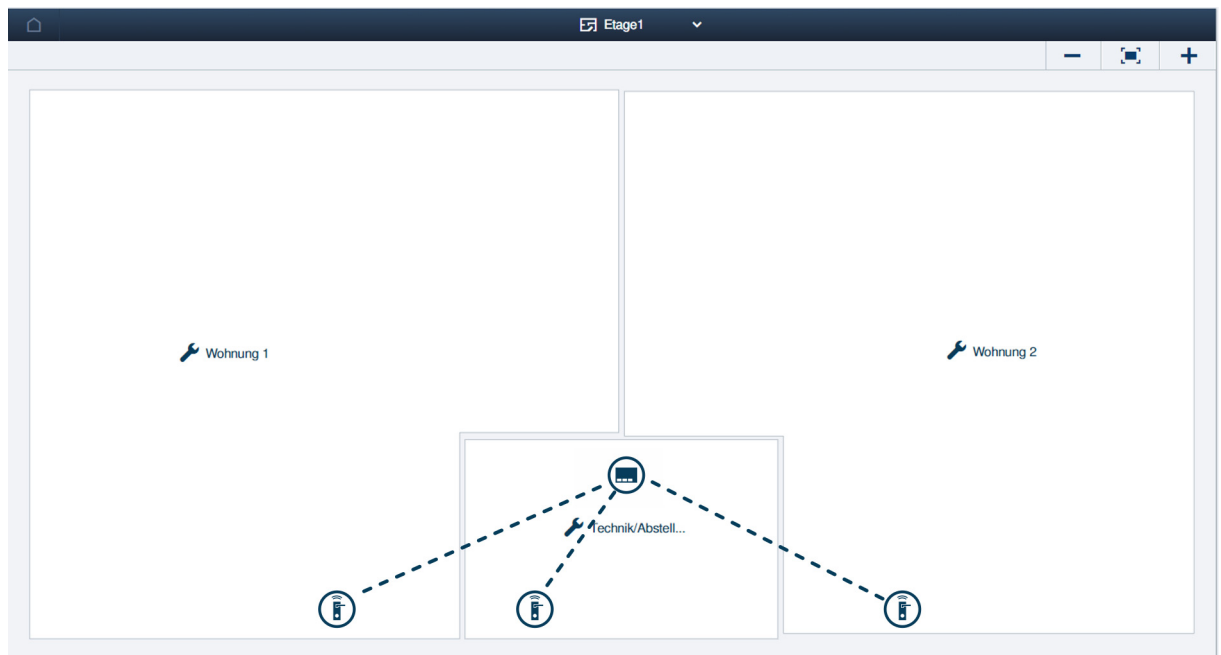


Abb. 53: Gebäudestruktur: Mehrfamilienhaus mit 3 „Elektronischer Schließzylinder“

Beispielaufbau einer Etage mit 2 Wohnungen eines Mehrfamilienhauses in der Verwaltungssoftware des „Smart Access Point Pro“. Die „Elektronischer Schließzylinder“ sind mit dem „Smart Access Point Pro“ verbunden.

- Informationen für die Erstellung einer Gebäudestruktur: siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95

4.3.3 Mehrfamilienhaus mit mehreren Geschossen

In einer Anlage „Busch-AccessControl“ werden in einem Mehrfamilienhaus der Haupteingang sowie die Wohnungseingänge mit „Elektronischer Schließzylinder“ ausgestattet.

Neben dem „Elektronischer Schließzylinder“ ist für die Benutzerverwaltung ein „Smart Access Point Pro“ erforderlich.

Durch die Geschossdecke wird die Reichweite der Funksignale stark reduziert. Für jedes weitere Geschoss ist daher der zusätzliche Einsatz eines RF/IP-Gateways für die Datenverteilung erforderlich.

- Die Anlage „Busch-AccessControl“ ist in diesem Beispiel nicht mit anderen Systemen vernetzt. Für den Einsatz eines RF/IP-Gateways ist ein PoE-Switch notwendig. Die Spannungsversorgung des „Smart Access Point Pro“ und des RF/IP-Gateways erfolgen über den PoE-Switch.

Die Entfernungen liegen innerhalb eines Geschosses innerhalb der Funkreichweite von etwa 10 Metern. Weitere Geräte zur Erhöhung der Reichweiten sind innerhalb der Geschosse daher nicht notwendig.

Nähere Informationen über die Kapazitäts- und Vernetzungsplanung finden Sie unter: siehe Kapitel 4.2 „Kapazität / Reichweite“ auf Seite 57.

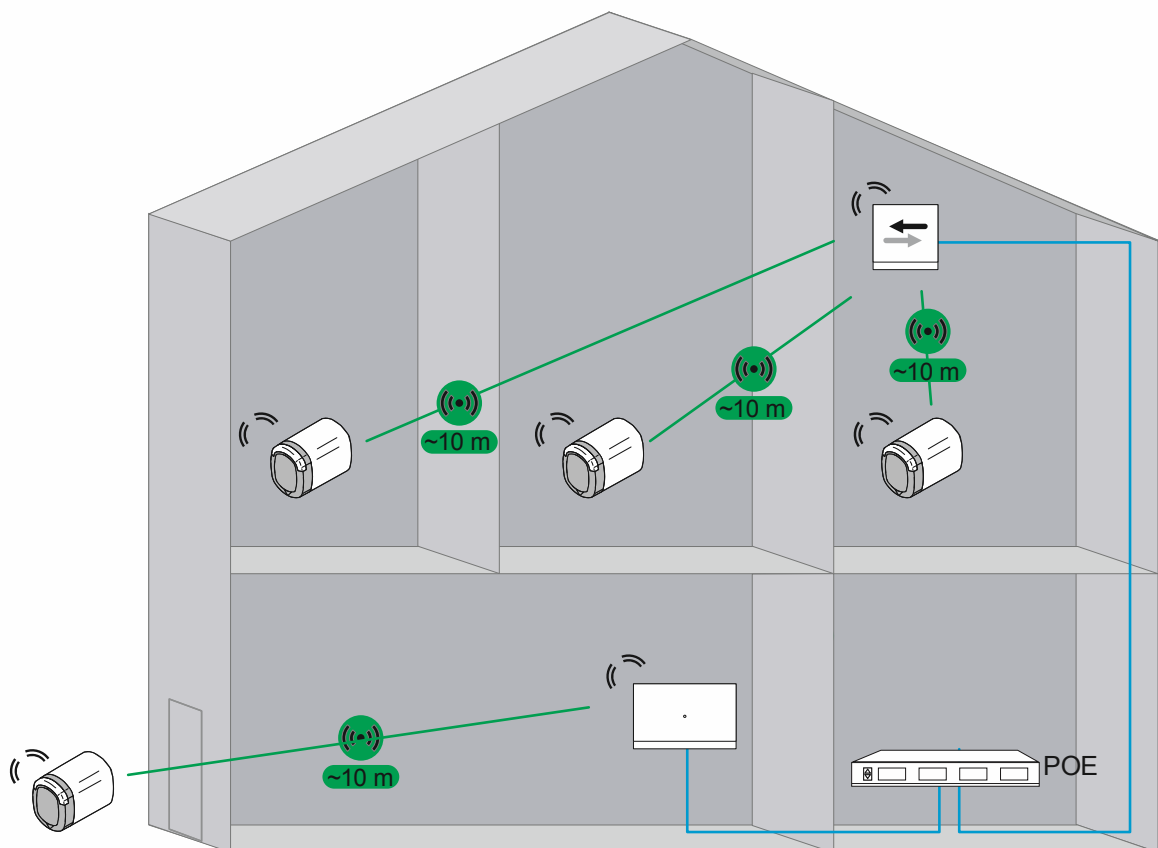


Abb. 54: Übersicht: Mehrfamilienhaus mit 4 „Elektronischer Schließzylinder“

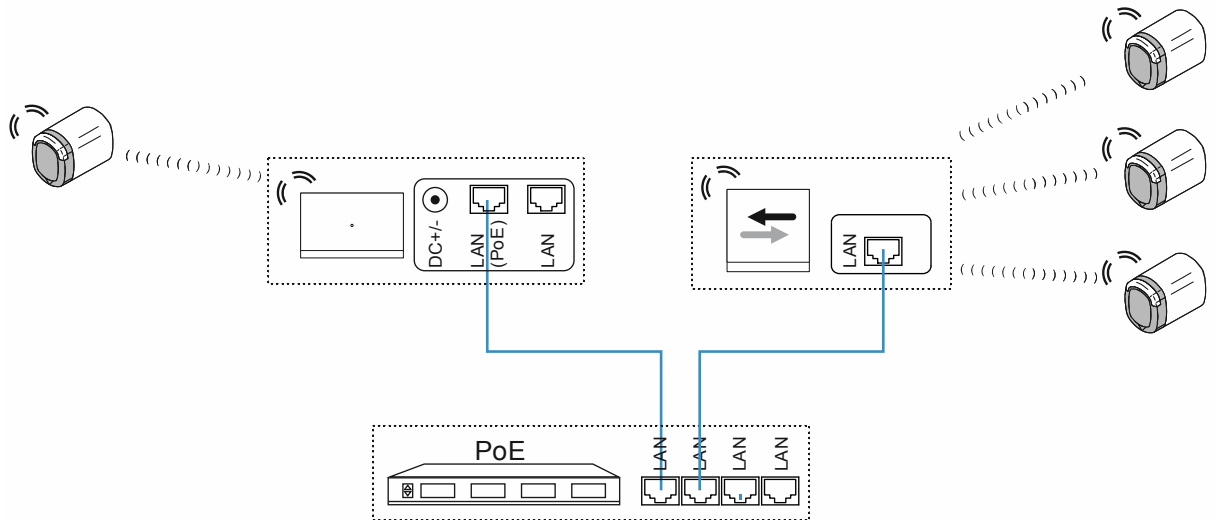


Abb. 55: Anschluss: Mehrfamilienhaus mit 4 „Elektronischer Schließzylinder“

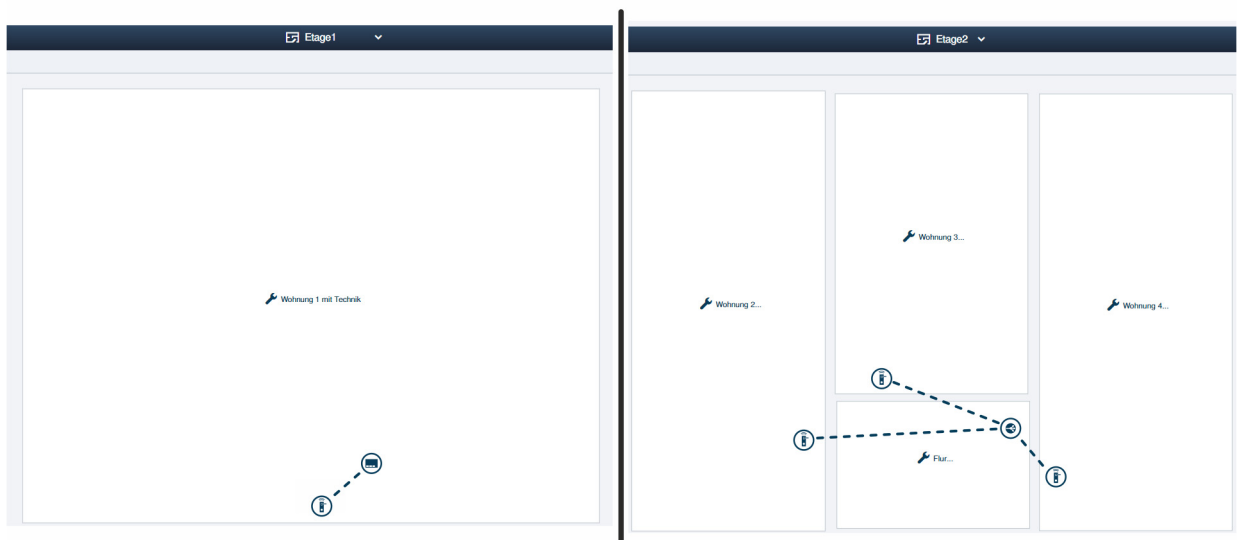


Abb. 56: Gebäudestruktur: Mehrfamilienhaus mit 4 „Elektronischer Schließzylinder“

Beispielaufbau der Wohnungen eines Mehrfamilienhauses in der Verwaltungssoftware des „Smart Access Point Pro“.

- Informationen für die Erstellung einer Gebäudestruktur: siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95

Etage 1:

Der „Elektronischer Schließzylinder“ ist mit dem „Smart Access Point Pro“ verbunden.

Etage 2:

Die „Elektronischer Schließzylinder“ sind mit dem RF/IP-Gateway verbunden.

4.3.4 Mehrfamilienhaus mit einer Arztpraxis

In einer Anlage „Busch-AccessControl“ werden in einem Mehrfamilienhaus der Haupteingang sowie die Wohnungseingänge mit „Elektronischer Schließzylinder“ ausgestattet.

In dem Gebäude befindet sich eine Arztpraxis. Für die Arztpraxis soll das Archiv im Keller ebenfalls mit einem „Elektronischer Schließzylinder“ ausgestattet werden. Zu diesem Raum besteht keine Funkverbindung.

Neben dem „Elektronischer Schließzylinder“ ist für die Benutzerverwaltung ein „Smart Access Point Pro“ erforderlich.

Durch die Geschossdecke wird die Reichweite der Funksignale stark reduziert. Für jedes weitere Geschoss ist daher der zusätzliche Einsatz eines RF/IP-Gateways für die Datenverteilung erforderlich.

- Der „Smart Access Point Pro“ ist in diesem Beispiel bereits vorhanden (z.B. in einer Installation „Busch-Welcome[®] IP“). Daher wird dieser mit genutzt. Die Spannungsversorgung des „Smart Access Point Pro“ und des RF/IP-Gateways erfolgt über den PoE-Switch.

Oberes Gebäude:

Die Entfernungen liegen innerhalb eines Geschosses innerhalb der Funkreichweite von etwa 10 Metern. Weitere Geräte zur Erhöhung der Reichweiten sind innerhalb der Geschosse daher nicht notwendig.

Nähere Informationen über die Kapazitäts- und Vernetzungsplanung finden Sie unter: siehe Kapitel 4.2 „Kapazität / Reichweite“ auf Seite 57.

Keller mit Archiv:

Die Installation einer Reichweitenerhöhung bis in den Keller ist nicht vorgesehen.

Da deshalb keine Funkverbindung zwischen dem „Elektronischer Schließzylinder“ und dem „Smart Access Point Pro“ besteht, muss für diesen Fall in der Benutzerverwaltung die Notfallfunktion für die infrage kommenden „Elektronischer Schließzylinder“ und zugehörigen Transponderschlüsseln eingerichtet werden. Mit der Notfallfunktion lässt sich das Archiv anschließend ohne Funkverbindung zum „Smart Access Point Pro“ öffnen und schließen.

- Für die Einrichtung der Notfallfunktion ist einmalig eine Funkverbindung des „Elektronischer Schließzylinder“ zum „Smart Access Point Pro“ erforderlich. Z.B. durch Demontage des Lesekopfes vom „Elektronischer Schließzylinder“. Für die Einrichtung der Notfallfunktion wird der Lesekopf dann in die Nähe des „Smart Access Point Pro“ gelegt.

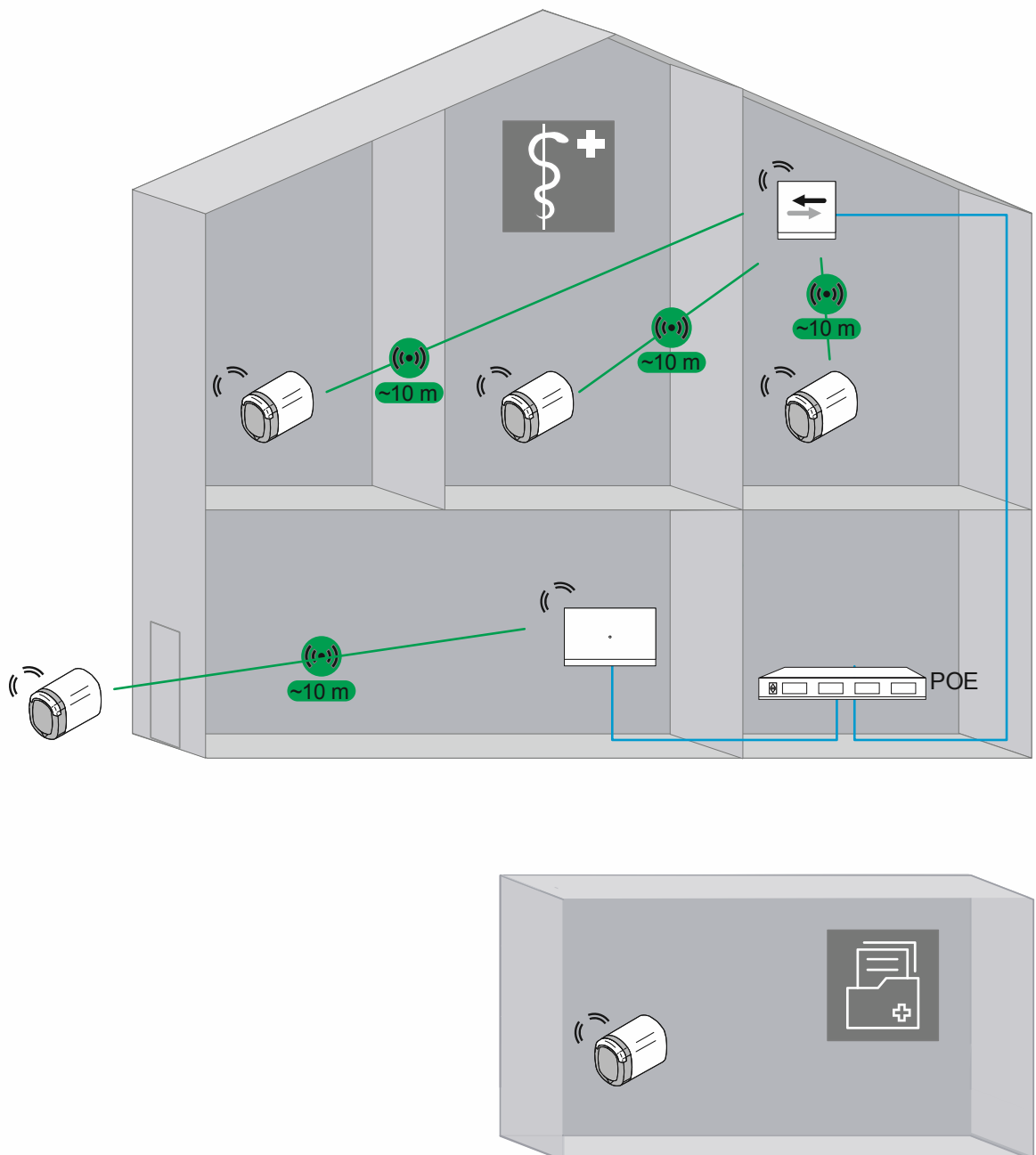


Abb. 57: Übersicht: Mehrfamilienhaus mit Arztpraxis und Archiv

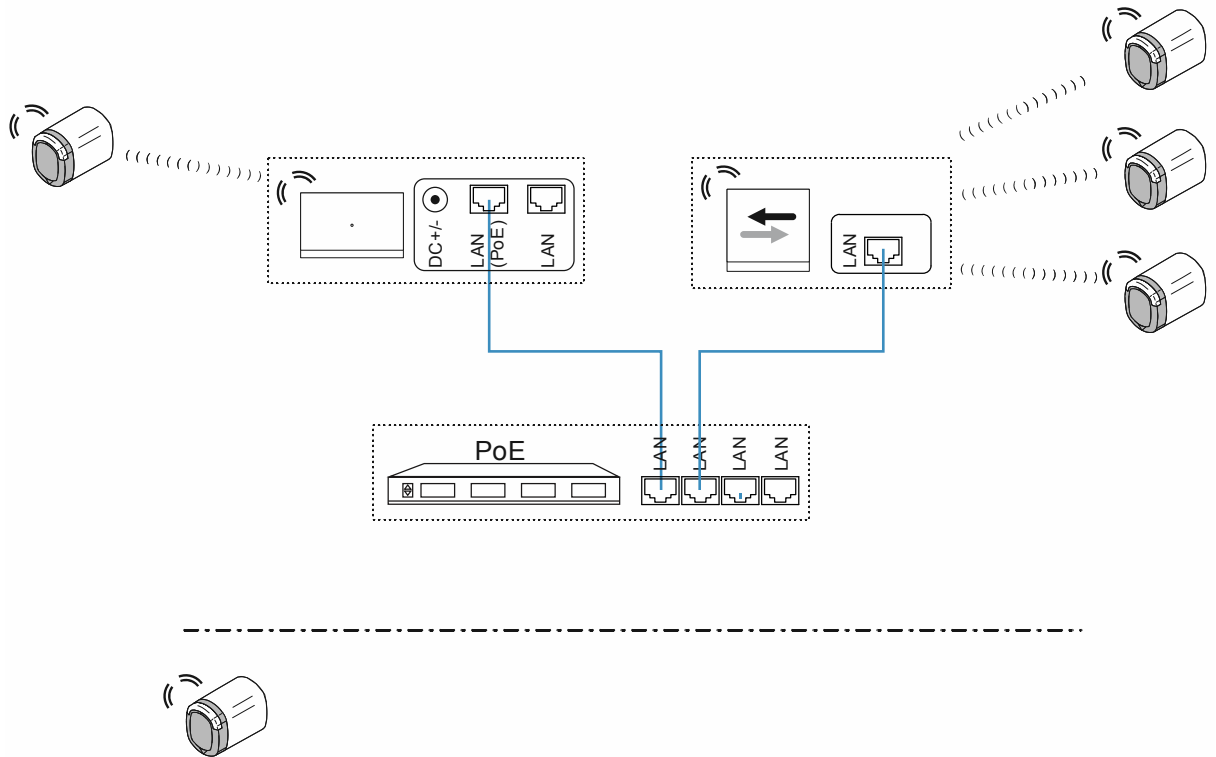


Abb. 58: Anschluss: Mehrfamilienhaus mit Arztpraxis und Archiv

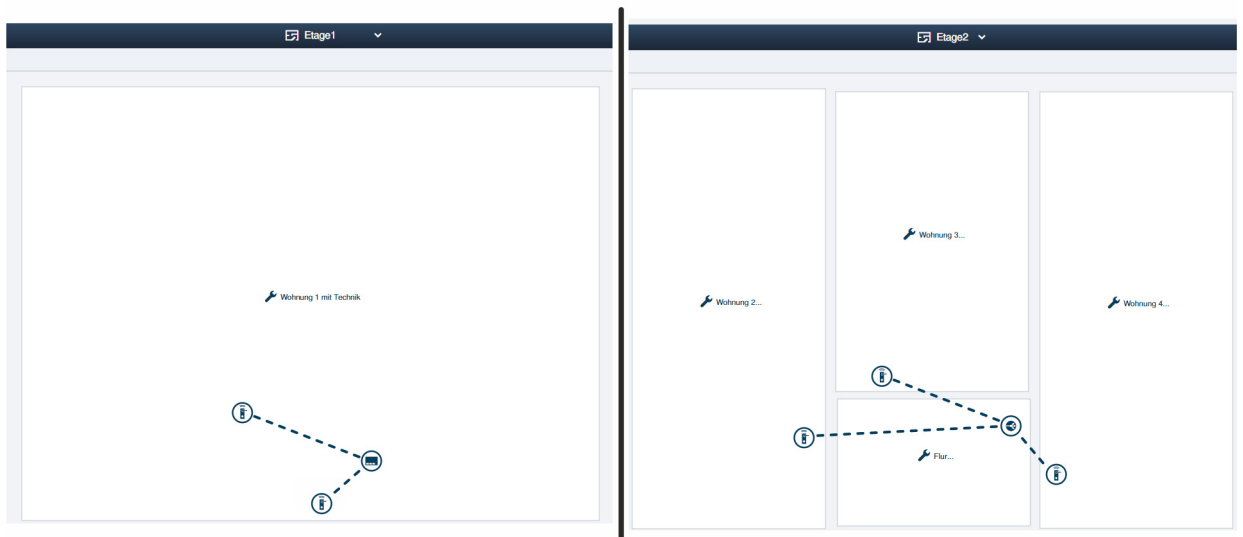


Abb. 59: Gebäudestruktur: Mehrfamilienhaus mit 4 „Elektronischer Schließzylinder“

Beispielaufbau der Wohnungen eines Mehrfamilienhauses in der Verwaltungssoftware des „Smart Access Point Pro“.

- Informationen für die Erstellung einer Gebäudestruktur: siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95

Etage 1:

Die „Elektronischer Schließzylinder“ sind mit dem „Smart Access Point Pro“ verbunden.

- Der „Elektronischer Schließzylinder“ für das Archiv wird als Gerät mit fehlender Verbindung markiert, sobald er sich für seinen Einsatz außerhalb der Reichweite des „Smart Access Point Pro“ befindet.

Etage 2:

Die „Elektronischer Schließzylinder“ sind mit dem RF/IP-Gateway verbunden.

4.3.5 Wohngebäude mit einem längeren Geschoss

In einer Anlage „Busch-AccessControl“ werden in einem eingeschossigen Wohngebäude der Haupteingang sowie die Wohnungseingänge mit „Elektronischer Schließzylinder“ ausgestattet.

Neben dem „Elektronischer Schließzylinder“ ist für die Benutzerverwaltung ein „Smart Access Point Pro“ erforderlich.

Durch Feuerschutzwände wird die Reichweite der Funksignale stark reduziert. Für jeden Bereich zwischen den Feuerschutzwänden ist daher der zusätzliche Einsatz eines RF/IP-Gateways für die Datenverteilung erforderlich.

- Die Anlage „Busch-AccessControl“ ist in diesem Beispiel nicht mit anderen Systemen vernetzt. Für den Einsatz eines RF/IP-Gateways ist ein PoE-Switch notwendig. Die Spannungsversorgung des „Smart Access Point Pro“ und des RF/IP-Gateways erfolgen über den PoE-Switch.

Die Entfernungen liegen innerhalb eines Bereiches innerhalb der Funkreichweite von etwa 10 Metern. Weitere Geräte zur Erhöhung der Reichweiten sind innerhalb dieser Bereiche daher nicht notwendig.

Nähere Informationen über die Kapazitäts- und Vernetzungsplanung finden Sie unter: siehe Kapitel 4.2 „Kapazität / Reichweite“ auf Seite 57.

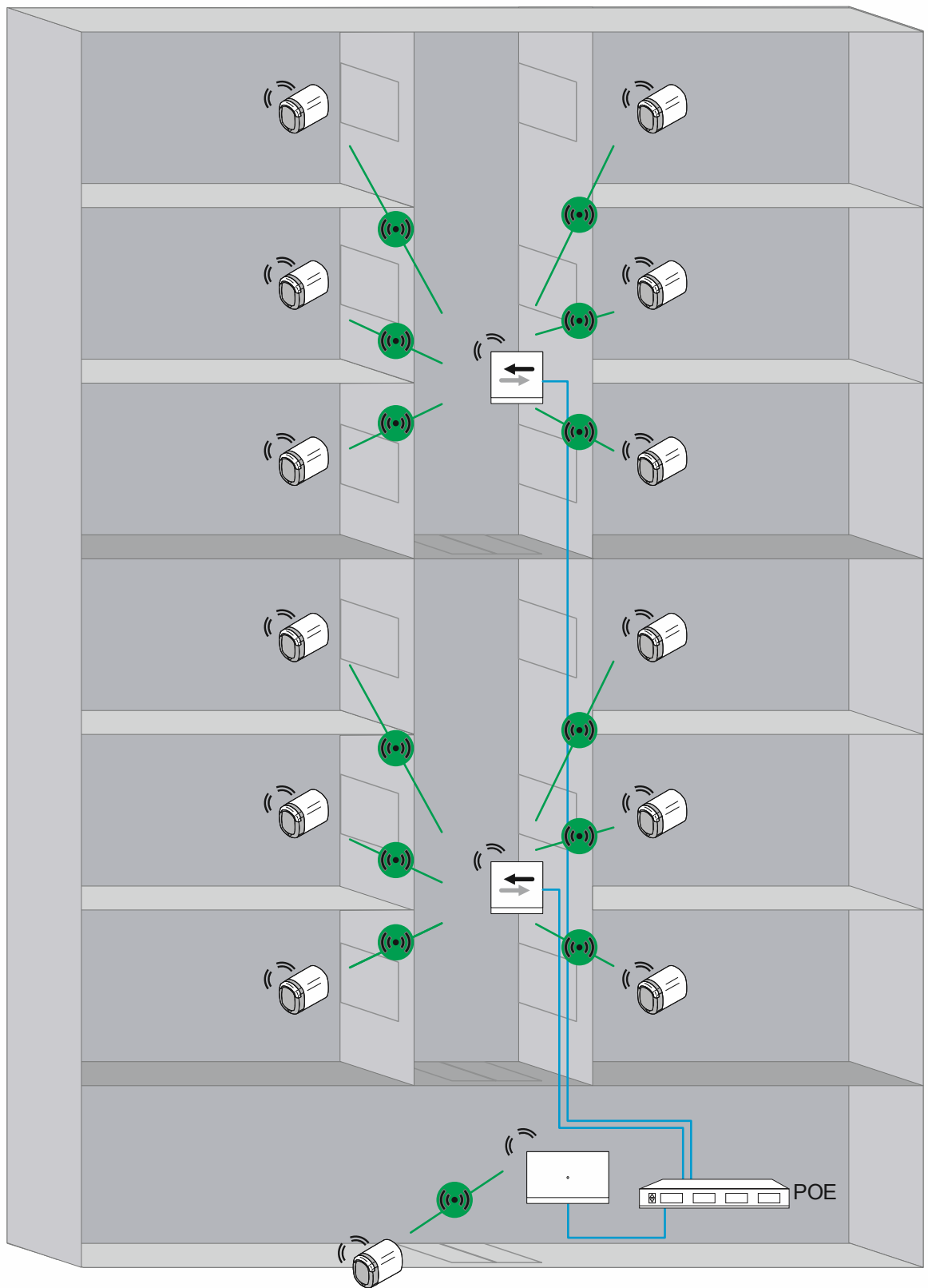


Abb. 60: Übersicht (Draufsicht): Wohngebäude mit mehr als 10 Meter Übertragungsstrecke und Funksignalhemmung durch Feuerschutzwände.

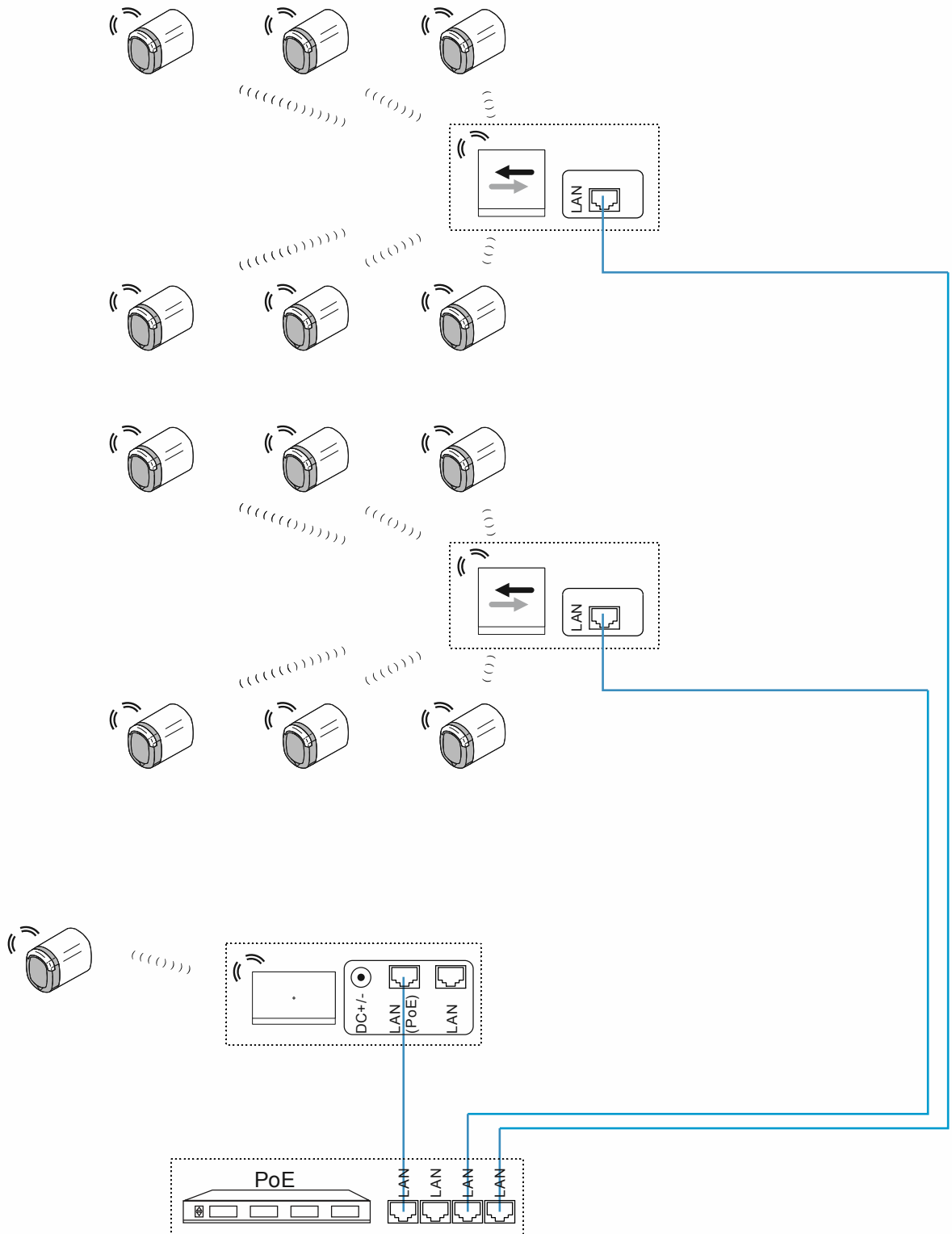


Abb. 61: Anschluss: Wohngebäude mit mehr als 10 Meter Übertragungsstrecke und Funksignalhemmung durch Feuerschutzwände.



Abb. 62: Gebäudestruktur: Wohngebäude mit mehr als 10 Meter Übertragungsstrecke und Funksignalhemmung durch Feuerschutzwände

Beispielaufbau der Wohnungen eines Mehrfamilienhauses in der Verwaltungssoftware des „Smart Access Point Pro“.

- Informationen für die Erstellung einer Gebäudestruktur: siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95

Haupteingang:

Der „Elektronischer Schließzylinder“ ist mit dem „Smart Access Point Pro“ verbunden.

Feuerschutzbereiche:

Die „Elektronischer Schließzylinder“ sind mit dem RF/IP-Gateway verbunden.

4.3.6 Wohngebäude mit mehreren Geschossen

In einer Anlage „Busch-AccessControl“ werden in einem mehrgeschossigen Wohngebäude der Haupteingang sowie die Wohnungseingänge mit „Elektronischer Schließzylinder“ ausgestattet.

Neben dem „Elektronischer Schließzylinder“ ist für die Benutzerverwaltung ein „Smart Access Point Pro“ erforderlich.

Durch die Geschossdecke wird die Reichweite der Funksignale stark reduziert. Für jedes weitere Geschoss ist daher der zusätzliche Einsatz eines RF/IP-Gateways für die Datenverteilung erforderlich.

- Die Anlage „Busch-AccessControl“ ist in diesem Beispiel nicht mit anderen Systemen vernetzt. Für den Einsatz eines RF/IP-Gateways ist ein PoE-Switch notwendig. Die Spannungsversorgung des „Smart Access Point Pro“ und des RF/IP-Gateways erfolgen über den PoE-Switch.

Die Entfernungen liegen innerhalb eines Geschosses oberhalb der Funkreichweite von etwa 10 Metern. Zur Erhöhung der Reichweiten kommen deshalb Repeater zum Einsatz.

- RF-Repeater sind nicht PoE-fähig. Sie benötigen eine gesonderte 24 V Spannungsversorgung.

Nähere Informationen über die Kapazitäts- und Vernetzungsplanung finden Sie unter: siehe Kapitel 4.2 „Kapazität / Reichweite“ auf Seite 57.

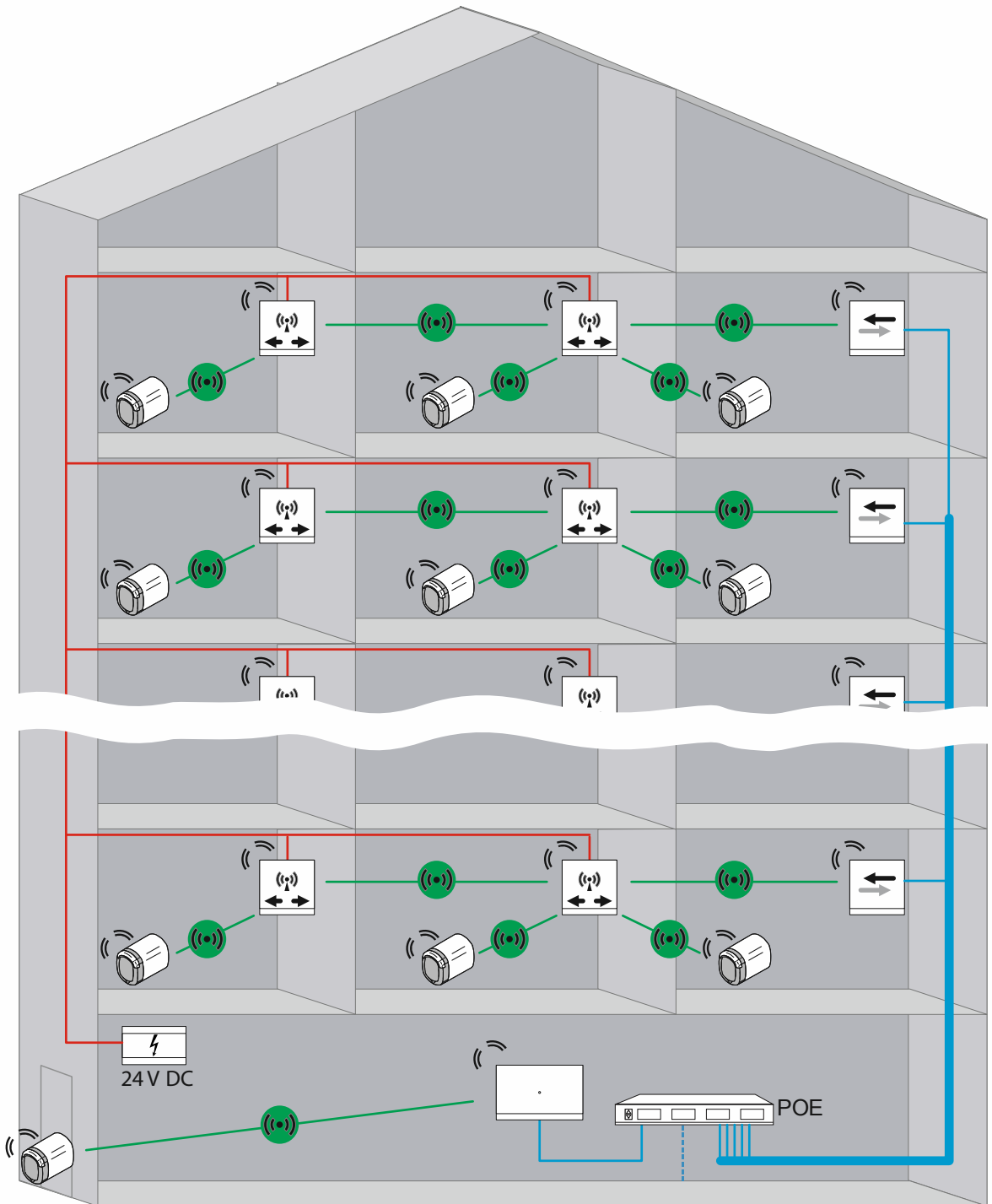


Abb. 63: Übersicht: Mehrgeschossiges Wohngebäude mit mehr als 10 Meter Übertragungsstrecke

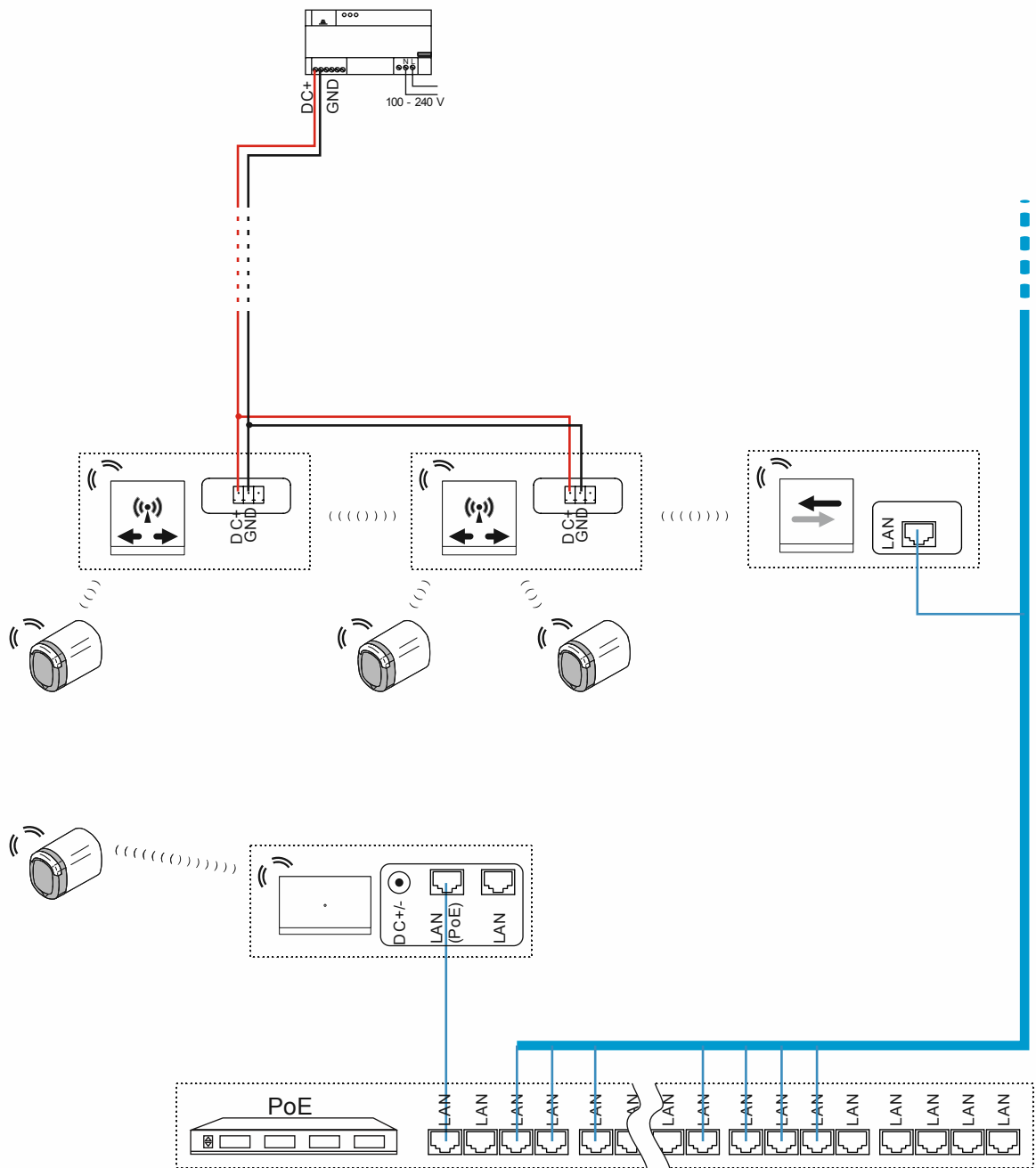


Abb. 64: Anschluss: Mehrgeschossiges Wohngebäude mit mehr als 10 Meter Übertragungsstrecke

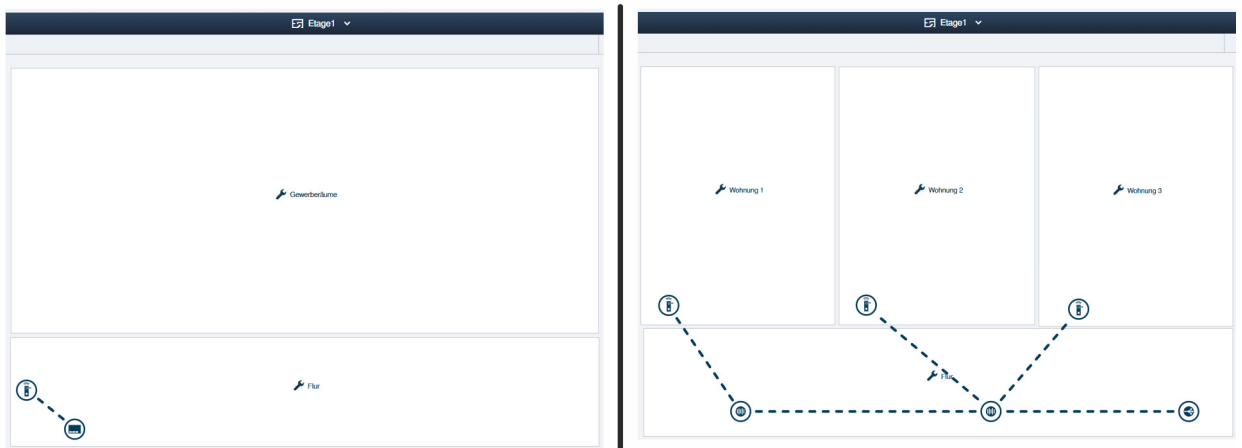


Abb. 65: Gebäudestruktur: Mehrgeschossiges Wohngebäude mit mehr als 10 Meter Übertragungsstrecke

Beispielaufbau der Wohnungen eines mehrstöckigen Mehrfamilienhauses mit mehr als 10 Meter Übertragungsstrecke innerhalb eines Geschosses in der Verwaltungssoftware des „Smart Access Point Pro“.

- Informationen für die Erstellung einer Gebäudestruktur: siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95

Etage 1:

Der „Elektronischer Schließzylinder“ ist mit dem „Smart Access Point Pro“ verbunden.

Etage 2 und weitere Etagen:

Die „Elektronischer Schließzylinder“ sind über Repeater mit dem RF/IP-Gateway verbunden.

4.3.7 Perimeter

In dem folgenden Beispiel wird eine Installation mit einem Perimeter dargestellt. Der Perimeter umfasst zwei Häuser und eine dazugehörige Parkgarage.

In der Anlage „Busch-AccessControl“ werden die Wohngebäude sowie die Parkgarage mit „Elektronischer Schließzylinder“ ausgestattet.

Neben den „Elektronischer Schließzylinder“ ist für die Benutzerverwaltung ein „Smart Access Point Pro“ erforderlich.

Die Signalverteilung in den weiteren Gebäuden und den jeweiligen Etagen übernehmen **RF/IP-Gateways**.

Für die Verbindung zwischen verschiedenen Gebäuden ist ein LAN-Netzwerk erforderlich. Die Spannungsversorgung der in diesem Beispiel eingesetzten Geräte erfolgt daher über PoE.

- In der Parkgarage sind in diesem Beispiel keine weiteren IP-Geräte in Betrieb. Der RF/IP-Repeater kann daher ohne einen gesonderten PoE-Switch betrieben werden.

Nähere Informationen über die Kapazitäts- und Vernetzungsplanung finden Sie unter: Kapitel 4.2 „Kapazität / Reichweite“ auf Seite 57.



Hinweis

Die Verbindung zwischen Häusern muss immer zwingend mit einem Glasfaserkabel erfolgen.

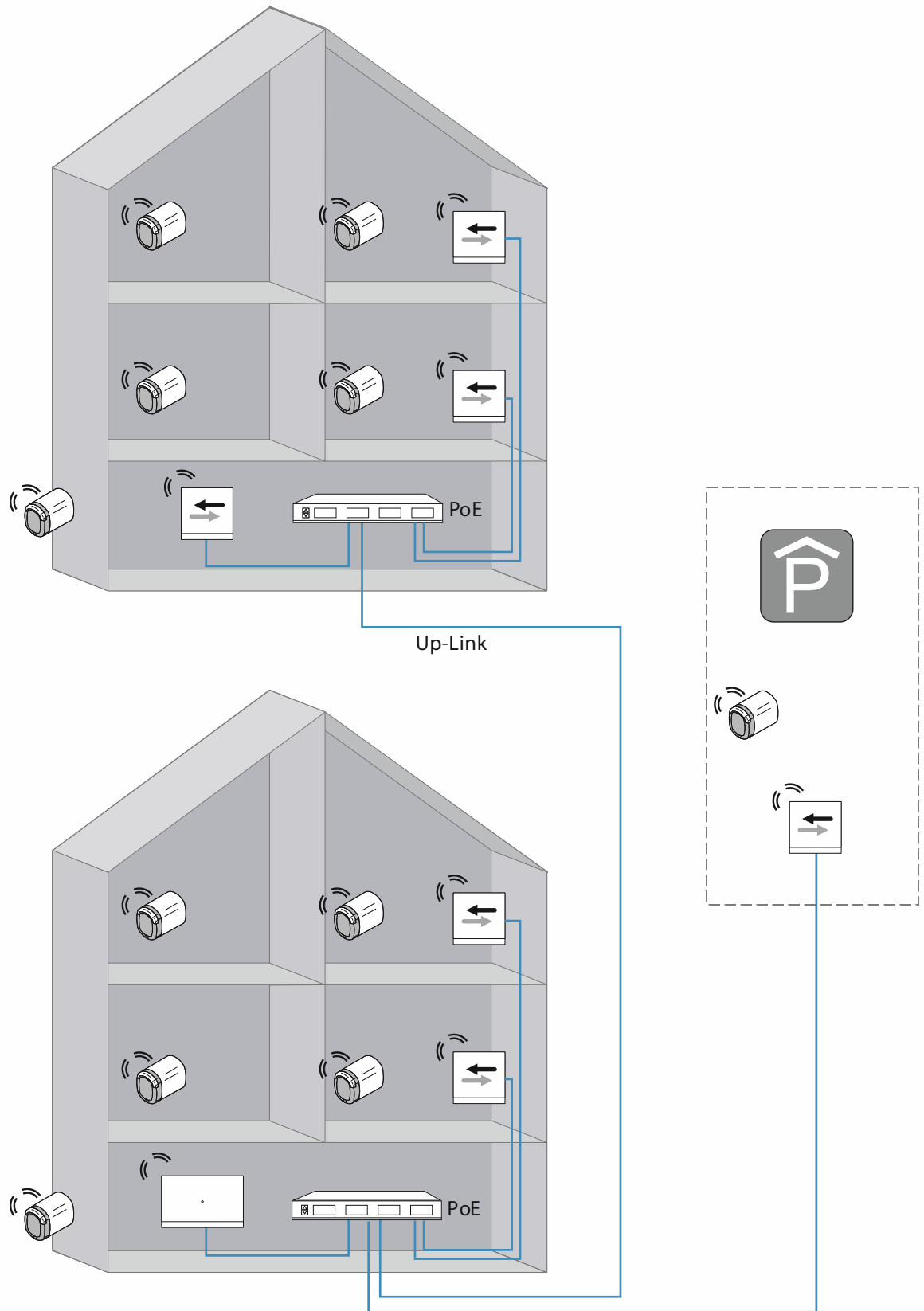


Abb. 66: Übersicht: Perimeter mit mehr als 40 Meter Übertragungsstrecke und weniger als 16 „Elektronischer Schließzylinder“

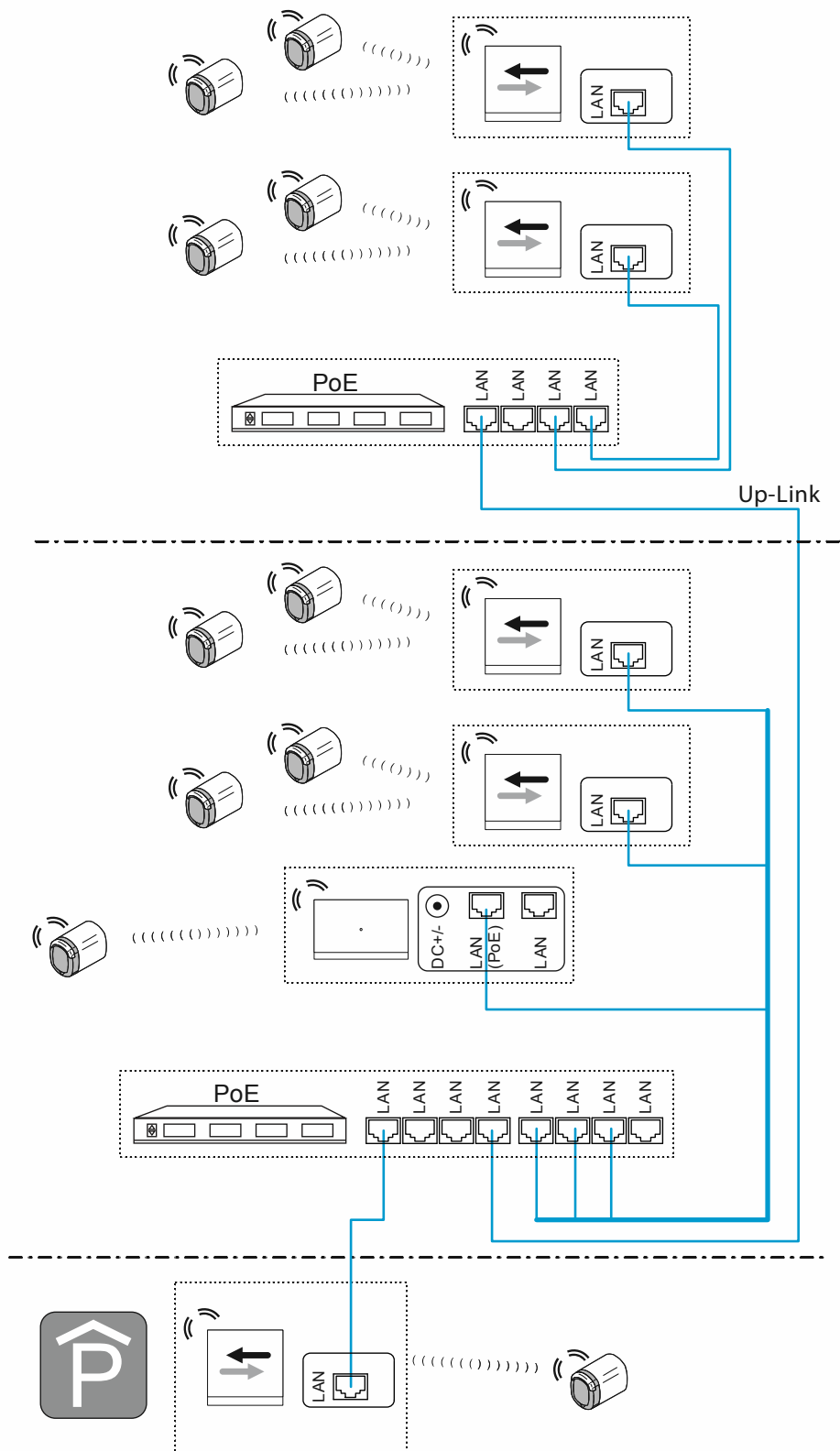


Abb. 67: Anschluss Perimeter mit mehr als 40 Meter Übertragungsstrecke und weniger als 16 „Elektronischer Schließzylinder“

UP-Link Verbindung für das Kaskadieren (Hintereinanderschalten) von Switchen:

- Besitzt der Switch einen Up-Link Anschluss:
Den Up-Link Anschluss mit einem normalen LAN-Kabel mit einem LAN-Anschluss des nächsten Switch verbinden.
- Besitzt der Switch keinen Up-Link Anschluss:
Einen LAN-Anschluss mit einem Crossover-Kabel mit einem LAN-Anschluss des nächsten Switch verbinden.



Achtung!

Fehlfunktionen

- Bei gebäudeübergreifender Verkabelung die Vorgaben der strukturierten Verkabelung beachten (Glasfaserleitung), siehe Kapitel 1.5 „Grundlagen strukturierter Verkabelung“ auf Seite 9.

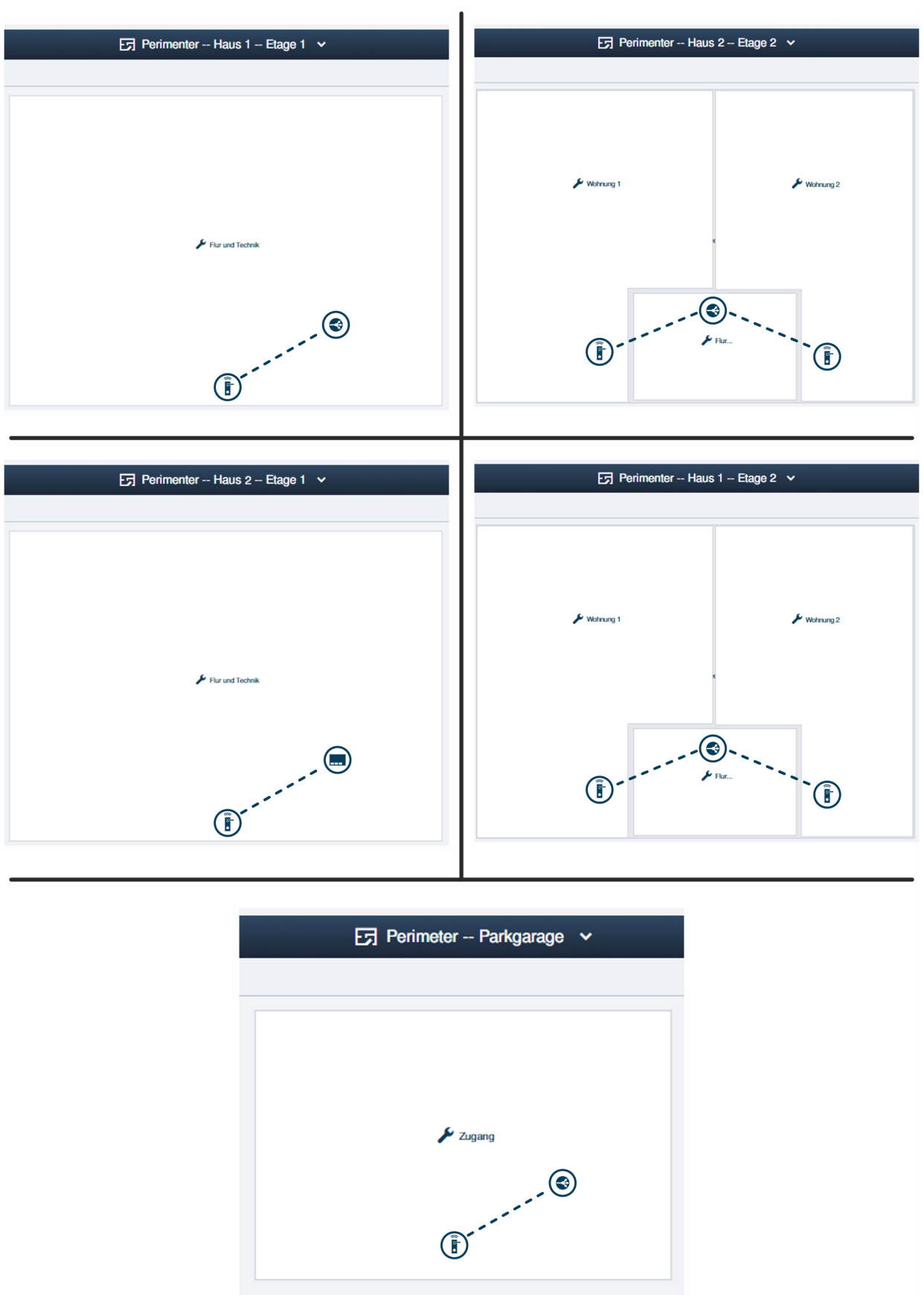


Abb. 68: Gebäudestruktur: Perimeter mit mehr als 40 Meter Übertragungsstrecke und weniger als 16 „Elektronischer Schließzylinder“

Beispielaufbau eines Systems mit mehreren Gebäuden inklusive einer Parkgarage in der Verwaltungssoftware des „Smart Access Point Pro“.

- Informationen für die Erstellung einer Gebäudestruktur: siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95

Gebäude 1 Etage 1:

Der „Elektronischer Schließzylinder“ ist mit dem RF/IP-Gateway verbunden.

Gebäude 1 Etage 2:

Die „Elektronischer Schließzylinder“ sind mit dem RF/IP-Gateway verbunden.

Gebäude 2 Etage 1:

Der „Elektronischer Schließzylinder“ ist mit dem „Smart Access Point Pro“ verbunden.

Gebäude 2 Etage 2:

Die „Elektronischer Schließzylinder“ sind mit dem RF/IP-Gateway verbunden.

Parkgarage:

Der „Elektronischer Schließzylinder“ ist mit dem RF/IP-Gateway verbunden.

4.4 Störquellen

Störungen zwischen Transponderschlüssel und Lesekey

Die Verbindung zwischen dem Lesekey des „Elektronischer Schließzylinder“ und dem Transponderschlüssel wird über die RFID-Technik durch Induktion ausgelöst.

Liegt der Transponderschlüssel beim Schaltvorgang des Lesekeys neben anderen Transponderschlüsseln oder RFID-Karten, kann es zu gegenseitigen Beeinflussungen kommen.

- Z.B. wenn der Transponderschlüssel mit anderen RFID-Karten im Geldbeutel aufbewahrt wird und der Geldbeutel vor den Lesekey gehalten wird.

Durch solche Beeinflussungen wird nichts zerstört. Es ist aber möglich, dass der Lesekey dann nicht schaltet.

Störungen der Kommunikation des Lesekeys mit der Verwaltungssoftware des „Smart Access Point Pro“

Die Kommunikation zwischen dem Lesekey und der Verwaltungssoftware des „Smart Access Point Pro“ erfolgt über die Frequenzen des Bluetooth.

- Störungen bei der Installation:
 - Die normale Reichweite von 10 Metern zwischen den einzelnen Geräten des „Busch-AccessControl“ wird durch die Gebäudestruktur beeinflusst. Müssen die Funksignale z.B. durch eine Stahlbetonwand, kann die Reichweite herabgesetzt sein.
- Störungen im laufenden Betrieb:
 - Die Geräte des „Busch-AccessControl“ sind fest installiert. Dadurch treten keine Probleme aufgrund von Standortänderungen auf.
 - Störungen können entstehen, wenn Fremdgeräte in der Nähe des Kommunikationsvorgangs auf denselben Frequenzen senden. Z.B. kabellose Telefone oder Mikrowellen. Es ist möglich, dass der Lesekey dann nicht schaltet. Wird die Störquelle aus dem Bereich behoben, funktioniert wieder alles wie gewohnt.

Neu montierte „Elektronischer Schließzylinder“ lassen sich nicht bedienen

- Der „Elektronischer Schließzylinder“ wurde an einem anderen Ort als dem Einsatzort in Betrieb genommen. Dadurch stimmt der Kommunikationspfad nicht mehr mit dem ursprünglichen überein. Der „Elektronischer Schließzylinder“ muss neu gekoppelt werden, siehe Kapitel 5.4.4 „Elektronischer Schließzylinder mit Smart Access Point koppeln“ auf Seite 112.
- Der „Elektronischer Schließzylinder“ wurde an einem neuen Ort montiert. Dadurch stimmt der Kommunikationspfad nicht mehr mit dem ursprünglichen überein. Der „Elektronischer Schließzylinder“ muss neu gekoppelt werden, siehe Kapitel 5.4.4 „Elektronischer Schließzylinder mit Smart Access Point koppeln“ auf Seite 112.

5 Verwaltungssoftware im „Smart Access Point Pro“

5.1 Übersicht

In der Verwaltungssoftware des „Smart Access Point Pro“ sind für das Einrichten und Verwalten des Zugangssystems Busch-AccessControl die folgenden Bereiche von Bedeutung.

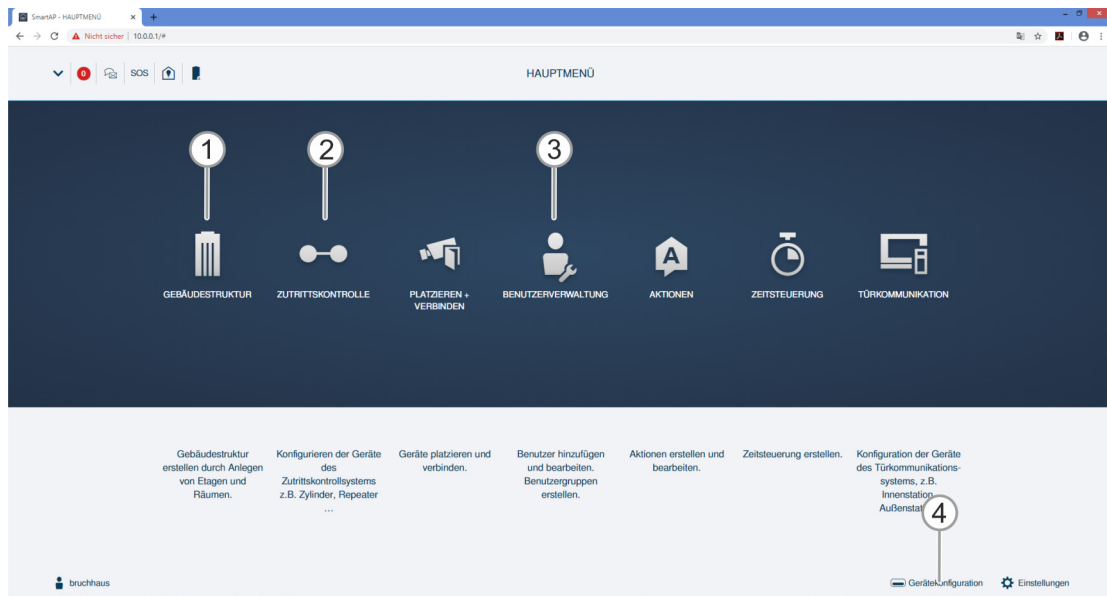


Abb. 69: Hauptmenü „Übersicht“

1 Gebäudestruktur

- Eine eingerichtete Gebäudestruktur ist Voraussetzung für das Platzieren und Koppeln von Geräten des Systems Busch-AccessControl.
- Zu den Funktionen im Bereich „Gebäudestruktur“, siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95.

2 Zutrittskontrolle

- Im Bereich „Zutrittskontrolle“ werden die Geräte des Systems Busch-AccessControl in der Gebäudestruktur platziert und miteinander gekoppelt.
- Zu den Funktionen im Bereich „Zutrittskontrolle“, siehe Kapitel 5.4 „Zutrittskontrolle“ auf Seite 103.

3 Benutzerverwaltung

- Im Bereich „Benutzerverwaltung“ werden die Schließrechte von Personen vergeben und verwaltet.
- Zu den Funktionen im Bereich „Benutzerverwaltung“, siehe Kapitel 5.5 „Benutzerverwaltung“ auf Seite 118.

4 Gerätekonfiguration

- Im Bereich „Gerätekonfiguration“ werden die Geräte des Systems Busch-AccessControl in der Verwaltungssoftware des „Smart Access Point Pro“ hinzugefügt.
- Nach dem Hinzufügen werden die Geräte des Systems Busch-AccessControl in den entsprechenden anderen Bereichen in der Gebäudestruktur platziert, gekoppelt und anschließend die Schließrechte vergeben.
- Zu den Funktionen im Bereich „Gerätekonfiguration“, siehe Kapitel 5.2 „Gerätekonfiguration“ auf Seite 87.

5.2 Gerätekonfiguration

Das Hinzufügen von Geräten erfolgt über den Menüpunkt „Gerätekonfiguration“ im Hauptmenü des „Smart Access Point Pro“.

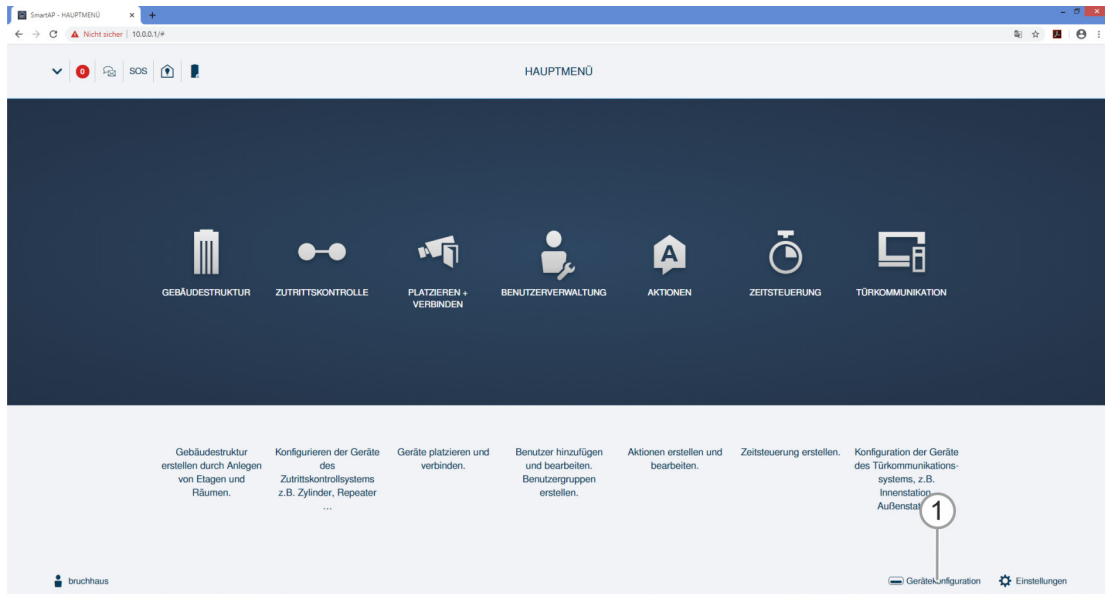


Abb. 70: Menü "Gerätekonfiguration"

Im Menüpunkt „Gerätekonfiguration“ [1] werden die folgenden Einstellungen vorgenommen:

- Geräte hinzufügen,
- Geräte aus dem System löschen,
- Geräteeigenschaften ändern.

5.2.1 „Smart Access Point Pro“ hinzufügen

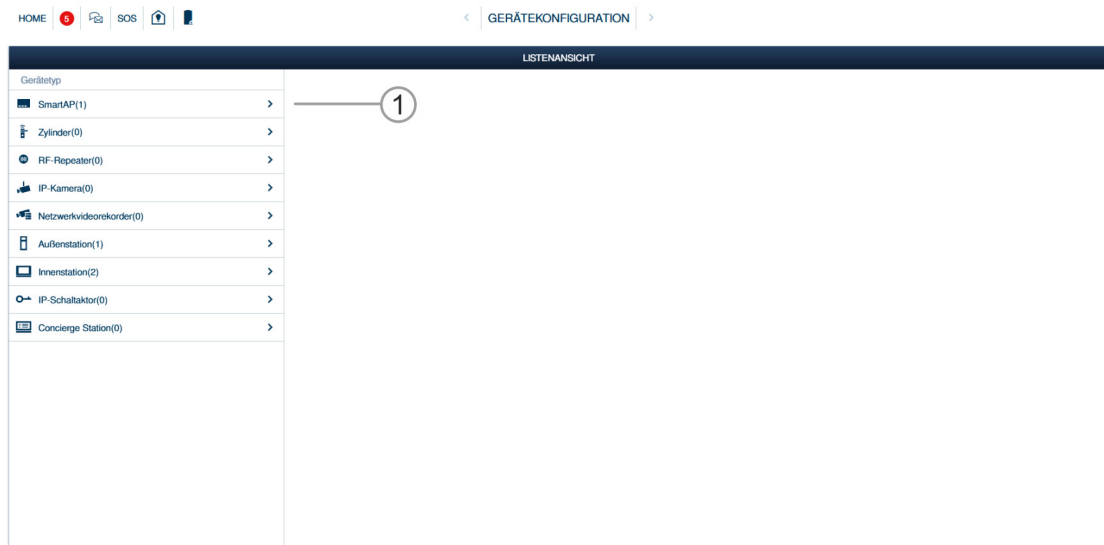


Abb. 71: „Smart Access Point Pro“ in der Liste der verfügbaren Geräte

Der „Smart Access Point Pro“ wird nicht hinzugefügt. Nach der Erstinbetriebnahme befindet sich der „Smart Access Point Pro“ automatisch in der Liste der verfügbaren Geräte [1].

5.2.2 „Elektronischer Schließzylinder“ hinzufügen

Führen Sie zum Hinzufügen eines „Elektronischer Schließzylinder“ die folgenden Schritte durch:



Abb. 72: Zylinder hinzufügen

1. Auf die Schaltfläche [1] „Zylinder“ klicken.

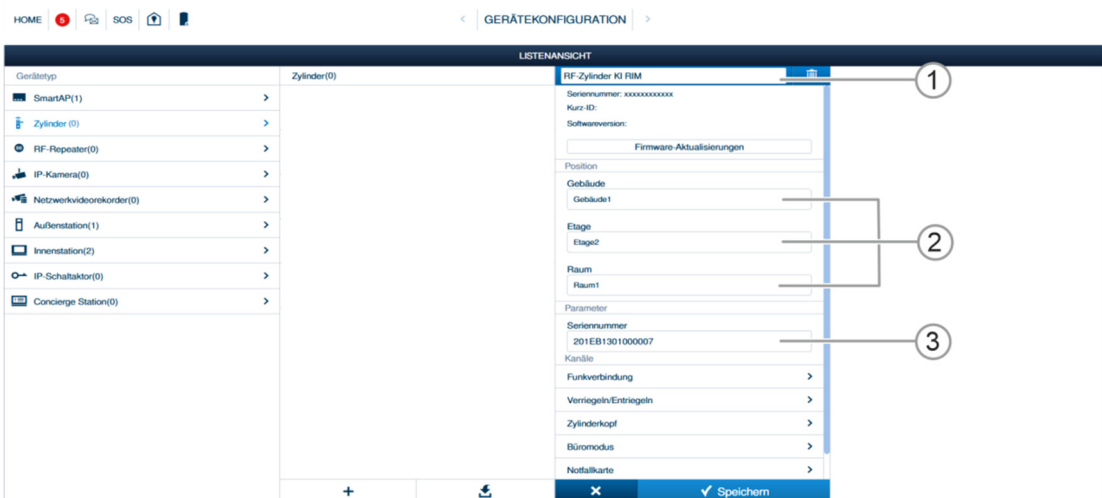


Abb. 73: Zylinderdaten eingeben

2. Den Namen des „Elektronischer Schließzylinder“ im Feld [1] eingeben.
3. Den „Elektronischer Schließzylinder“ zur Gebäudestruktur [2] zuordnen (Gebäude, Etage, Raum).
 - Die Zuordnung zur Gebäudestruktur kann auch zu einem späteren Zeitpunkt erfolgen siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95.
4. Seriennummer [3] des „Elektronischer Schließzylinder“ eingeben.
 - Die Seriennummer befindet sich auf dem Typenschild im Batteriefach, siehe Kapitel 3.2.1 „„Elektronischer Schließzylinder“““ auf Seite 43.
5. Schaltfläche „Speichern“ klicken.



Abb. 74: „Elektronischer Schließzylinder“ angelegt

Der angelegte „Elektronischer Schließzylinder“ wird im Feld [1] „Zylinder“ angezeigt.

5.2.3 „RF/IP Gateway“ hinzufügen

Führen Sie zum Hinzufügen eines „RF/IP Gateway“ die folgenden Schritte durch:

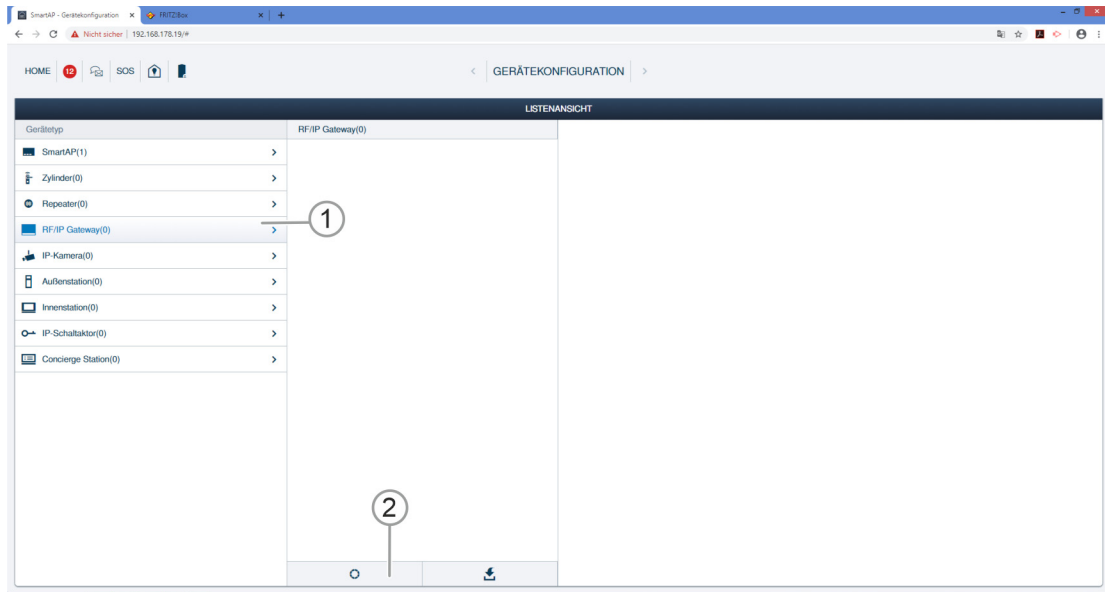


Abb. 75: IP-Gateway hinzufügen

1. Auf die Schaltfläche „RF/IP Gateway“ [1] klicken.
2. Auf die Schaltfläche „Suche“ [2] klicken.

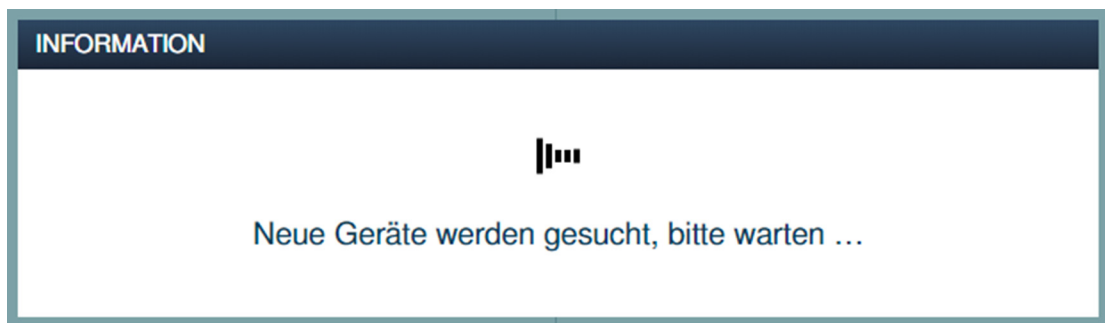


Abb. 76: „RF/IP Gateway“ Suche

- Das System sucht nach erreichbaren „RF/IP Gateway“.

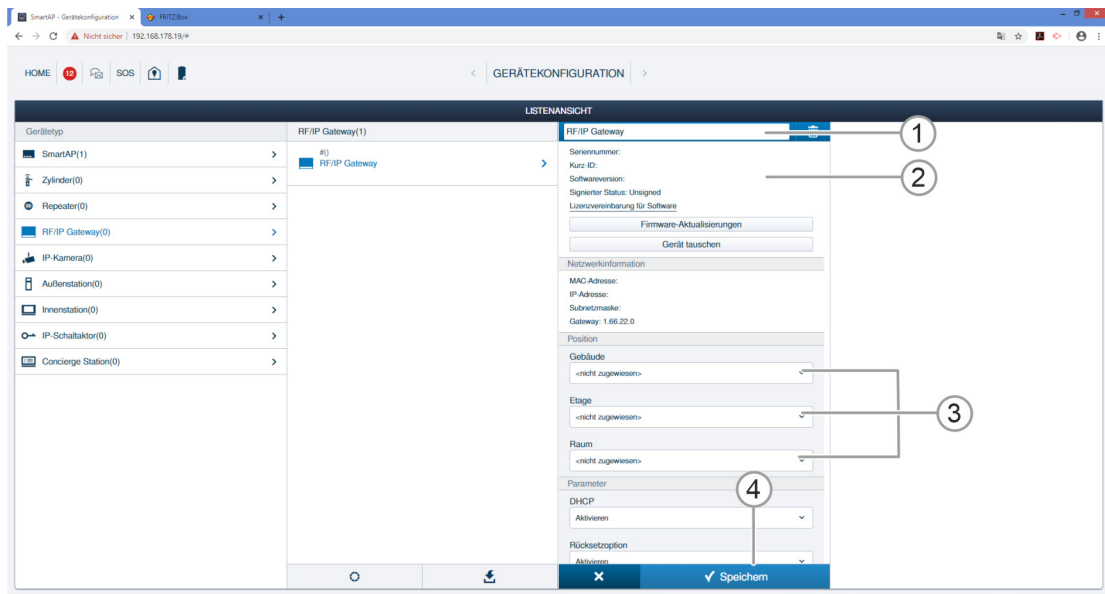


Abb. 77: IP-Gateway Eigenschaften

- Alle gefundenen „RF/IP Gateway“ werden in der Listenansicht angezeigt.
3. Den Namen des „RF/IP Gateway“ im Feld [1] eingeben.
 4. Seriennummer [2] des „RF/IP Gateway“ eingeben.
 5. Den „RF/IP Gateway“ zur Gebäudestruktur [3] zuordnen (Gebäude, Etage, Raum).
 - Die Zuordnung zur Gebäudestruktur kann auch zu einem späteren Zeitpunkt erfolgen siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95.
 6. Schaltfläche „Speichern“ [4] klicken.
- Der „RF/IP Gateway“ ist angelegt.

5.2.4 „RF Repeater“ hinzufügen

Führen Sie zum Hinzufügen eines „RF Repeater“ die folgenden Schritte durch:

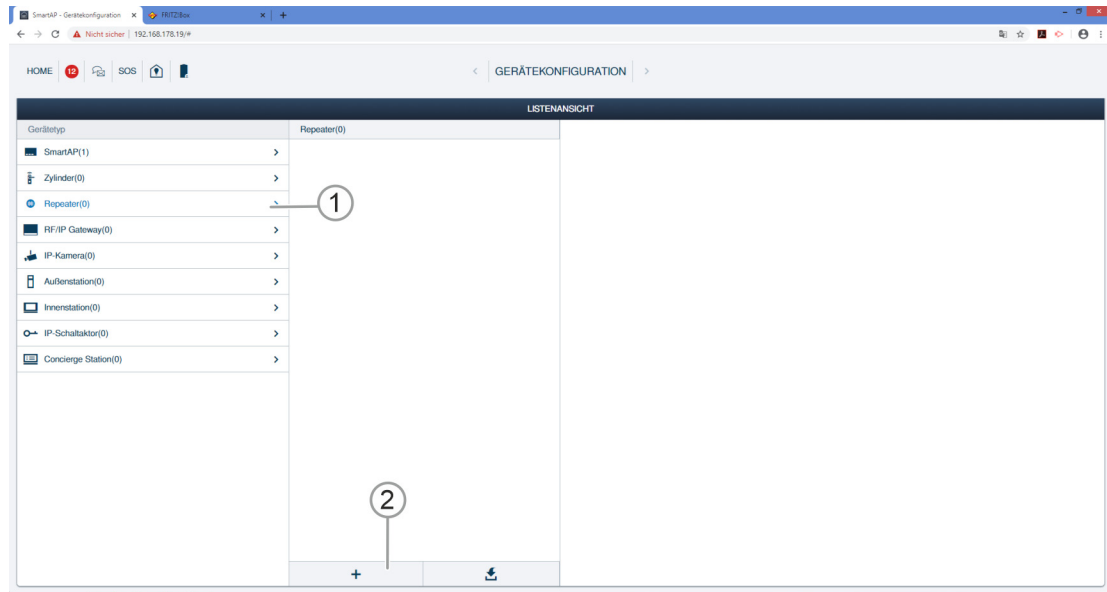


Abb. 78: „RF Repeater“ hinzufügen

1. Auf die Schaltfläche „RF Repeater“ [1] klicken.
2. Schaltfläche „Hinzufügen“ [2] klicken.

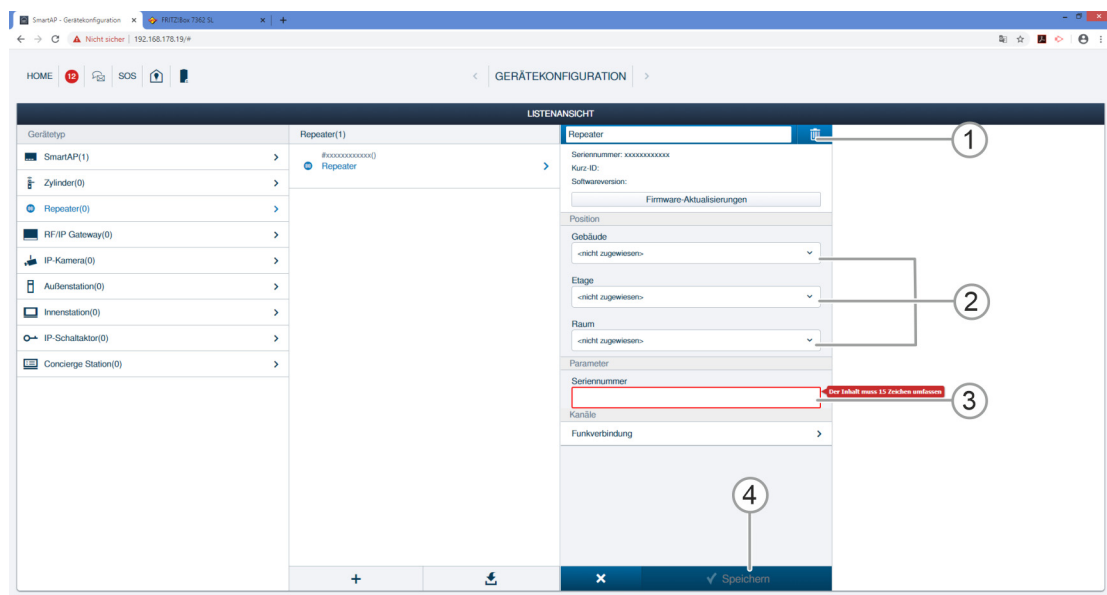


Abb. 79: Eigenschaften „RF Repeater“

3. Den Namen des „RF Repeater“ im Feld [1] eingeben.

4. Den „RF Repeater“ zur Gebäudestruktur [2] zuordnen (Gebäude, Etage, Raum).
 - Die Zuordnung zur Gebäudestruktur kann auch zu einem späteren Zeitpunkt erfolgen siehe Kapitel 5.3 „Gebäudestruktur“ auf Seite 95.
5. Seriennummer [3] des „RF Repeater“ eingeben.
6. Schaltfläche „Speichern“ [4] klicken.

Der „RF Repeater“ ist angelegt.

5.3 Gebäudestruktur

Das Erstellen von Gebäuden, Etagen und Räumen erfolgt über den Menüpunkt „Gebäudestruktur“ im Hauptmenü des „Smart Access Point Pro“.

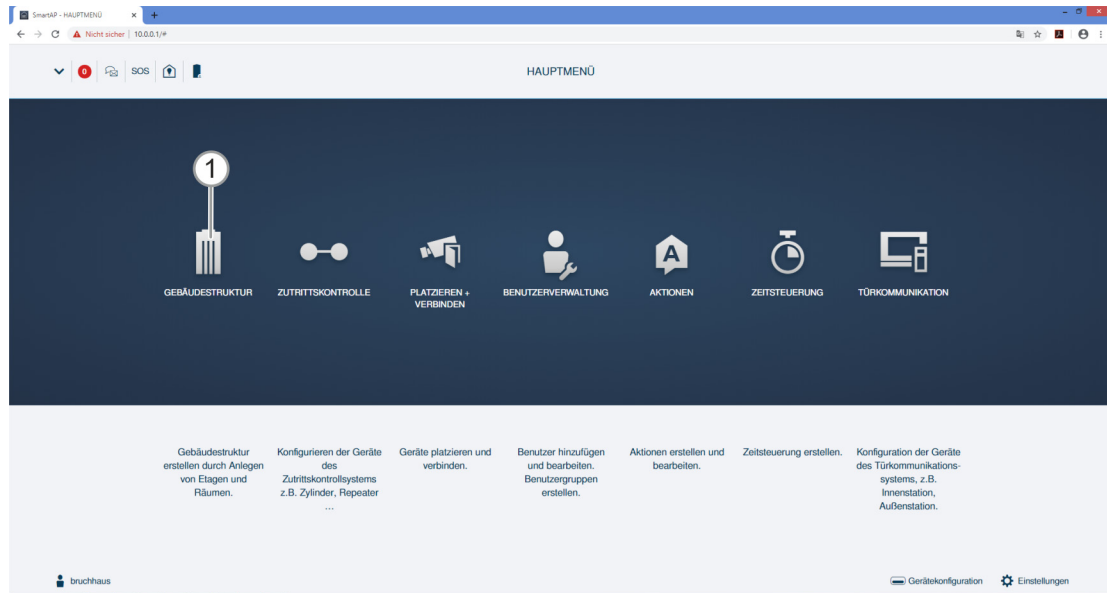


Abb. 80: Menü "Gebäudestruktur"

Im Menüpunkt „Gebäudestruktur“ werden die folgenden Einstellungen vorgenommen:

- Gebäude hinzufügen
- Etagen hinzufügen
- Räume hinzufügen

5.3.1 Gebäude anlegen

Führen Sie zum Anlegen des Gebäudes die folgenden Schritte durch:

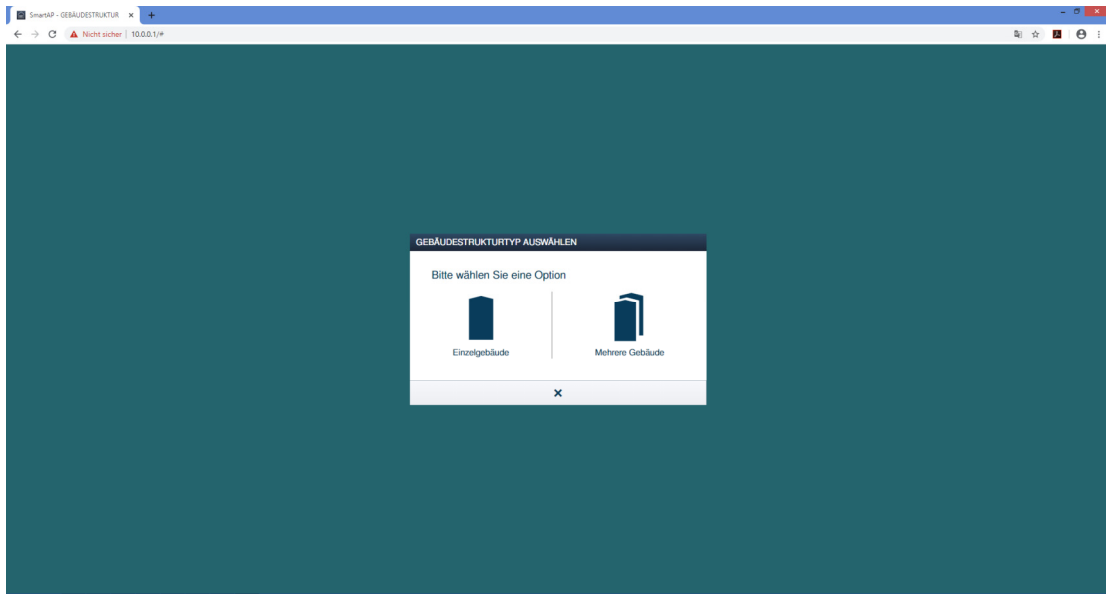


Abb. 81: Auswahl Gebäudestrukturtyp

1. Im Fenster „Gebäudestrukturtyp“ auswählen, ob es sich um ein „Einzelgebäude“ oder „Mehrere Gebäude“ handelt.

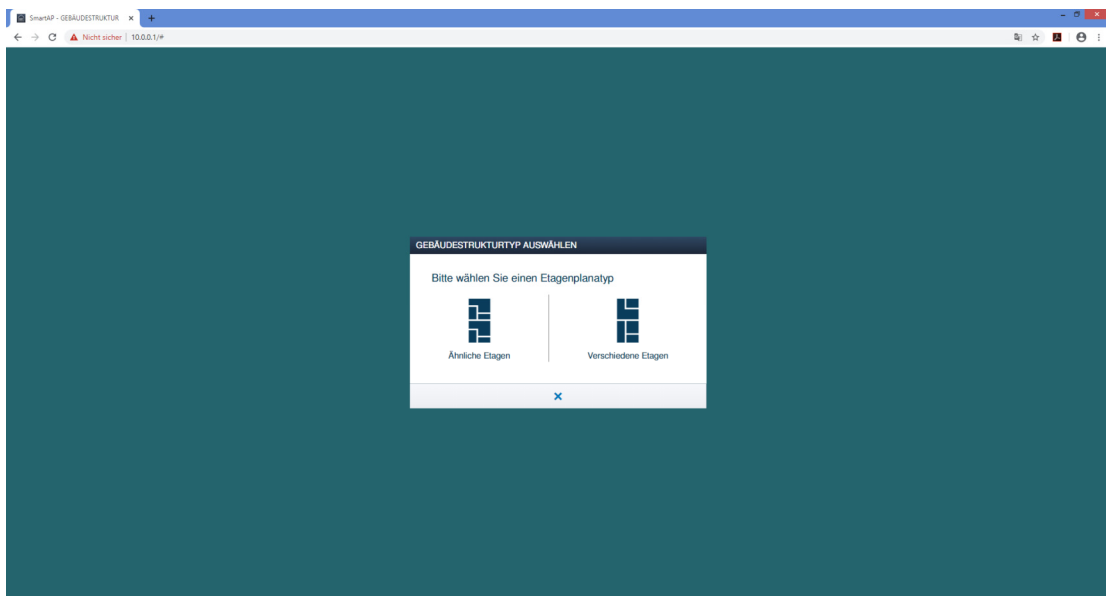


Abb. 82: Etagenplantyp auswählen

2. Im Fenster „Etagenplantyp“ auswählen, ob die Etagen einen ähnlichen oder verschiedenen Grundriss aufweisen.

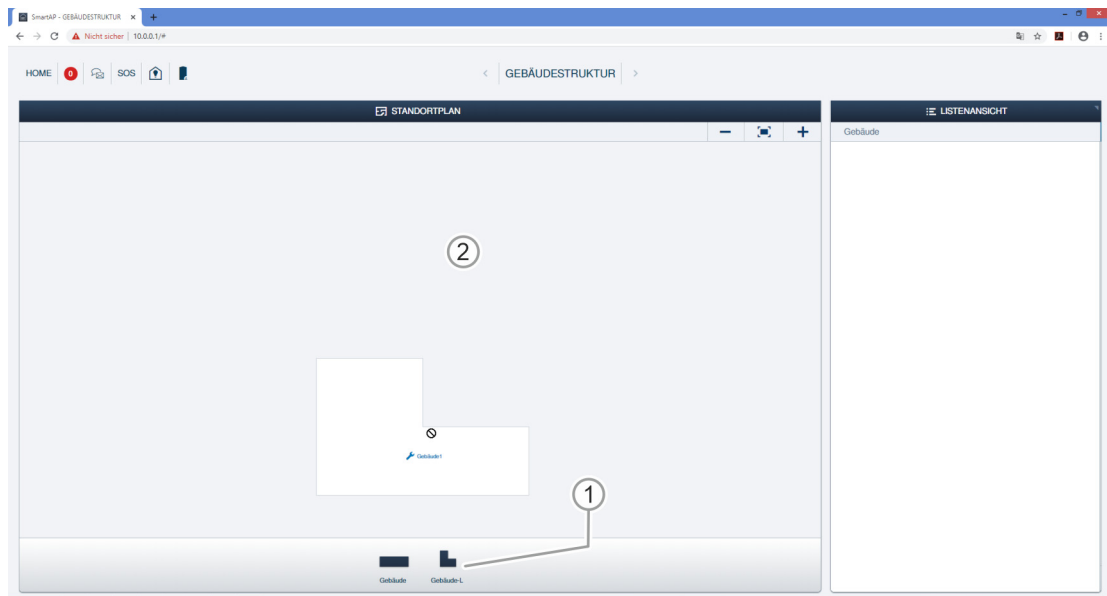


Abb. 83: Gebäudeform auswählen

3. Passende Gebäudeform aus der Liste [1] auswählen und auf die Arbeitsfläche [2] ziehen.

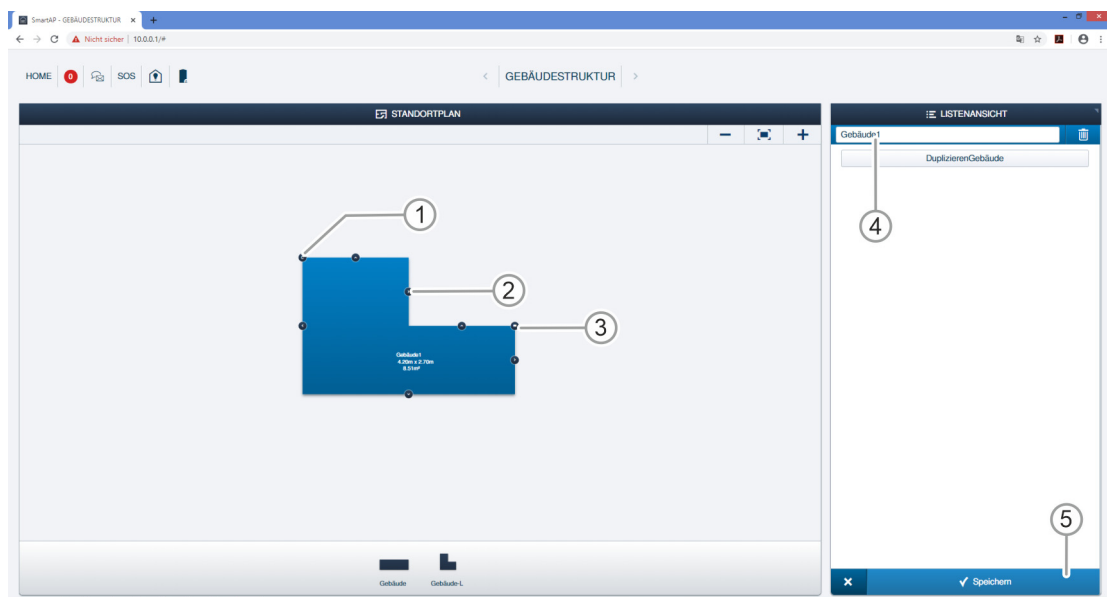


Abb. 84: Gebäudeform anpassen

4. Gebäude anklicken.
 - Das Gebäude wird blau hinterlegt. Am Rand des Gebäudes erscheinen Schaltflächen, mit denen das Gebäude in Form und Größe verändert werden kann:
 - Mit Schaltfläche [1] wird das Gebäude gedreht.
 - Mit Schaltfläche [2] wird die Position der einzelnen Kanten verändert.
 - Mit Schaltfläche [3] wird das Gebäude vergrößert oder verkleinert.
5. Gebäudenamen im Feld [4] eintragen.
6. Schaltfläche „Speichern“ [5] klicken.

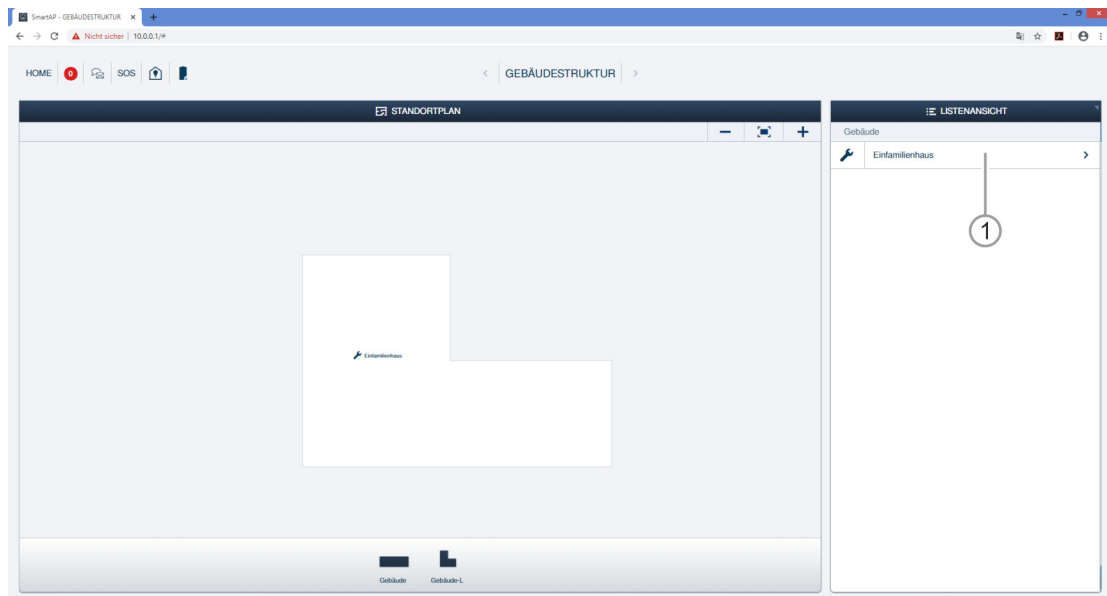


Abb. 85: Gebäude zur weiteren Bearbeitung auswählen.

- Auf den Gebäudenamen in der Liste [1] klicken, um das Gebäude zur weiteren Bearbeitung auszuwählen.

5.3.2 Etagen anlegen

Führen Sie zum Anlegen der Etagen die folgenden Schritte durch:

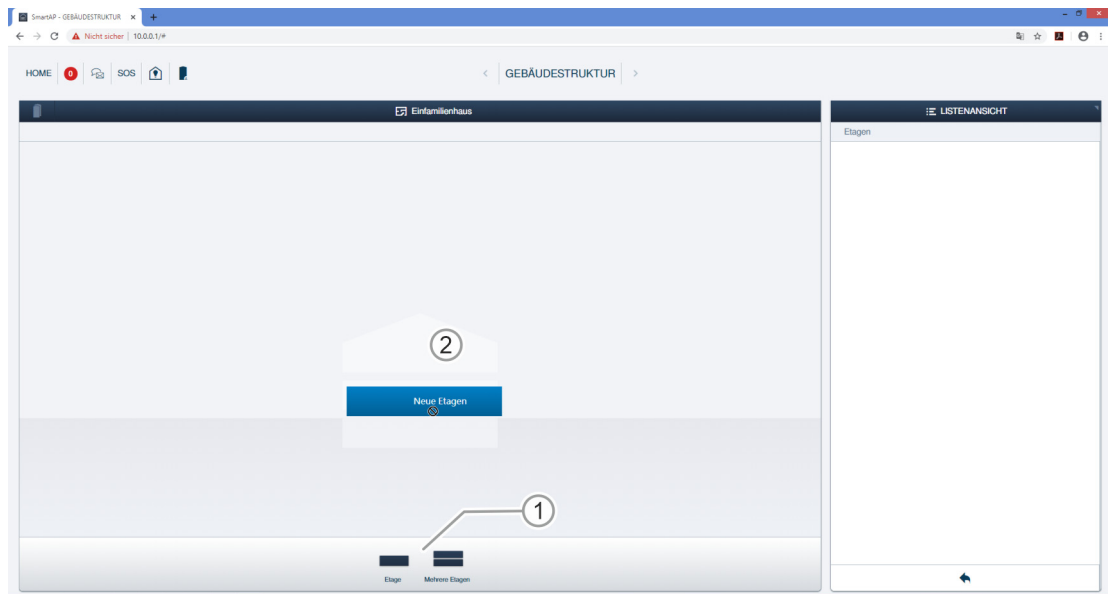


Abb. 86: Etagenvariante wählen

1. Etagenvariante aus Liste [1] auswählen und auf das Gebäude [2] ziehen.

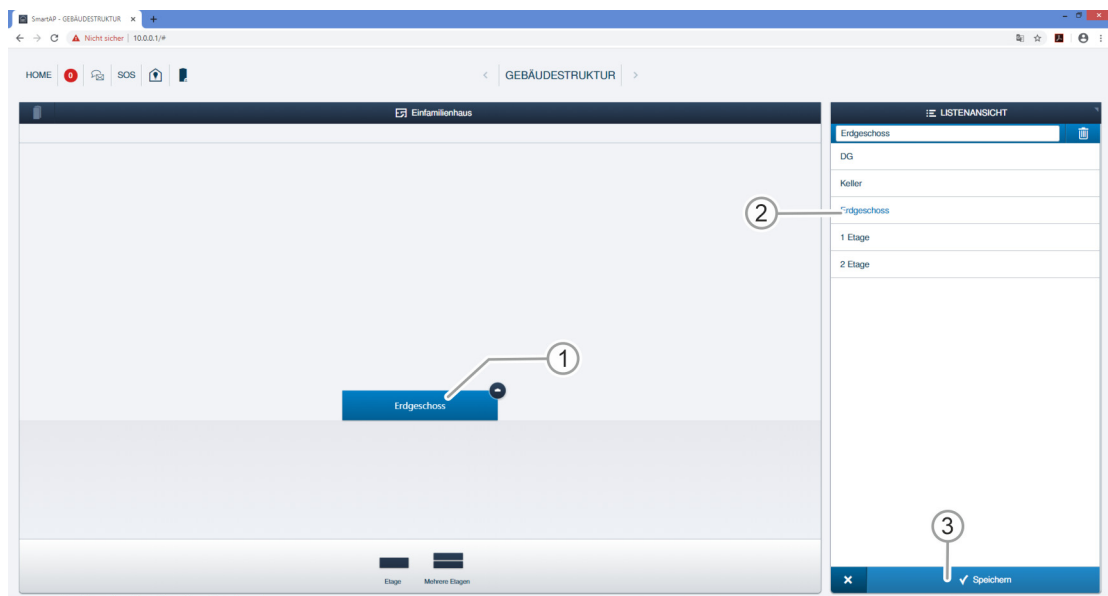


Abb. 87: Etageigenschaften

2. Etage [1] anklicken.
3. Etagentyp aus der Liste [2] auswählen und auf die Schaltfläche „Speichern“ [3] klicken.
4. Ggfs. weitere Etagen hinzufügen.

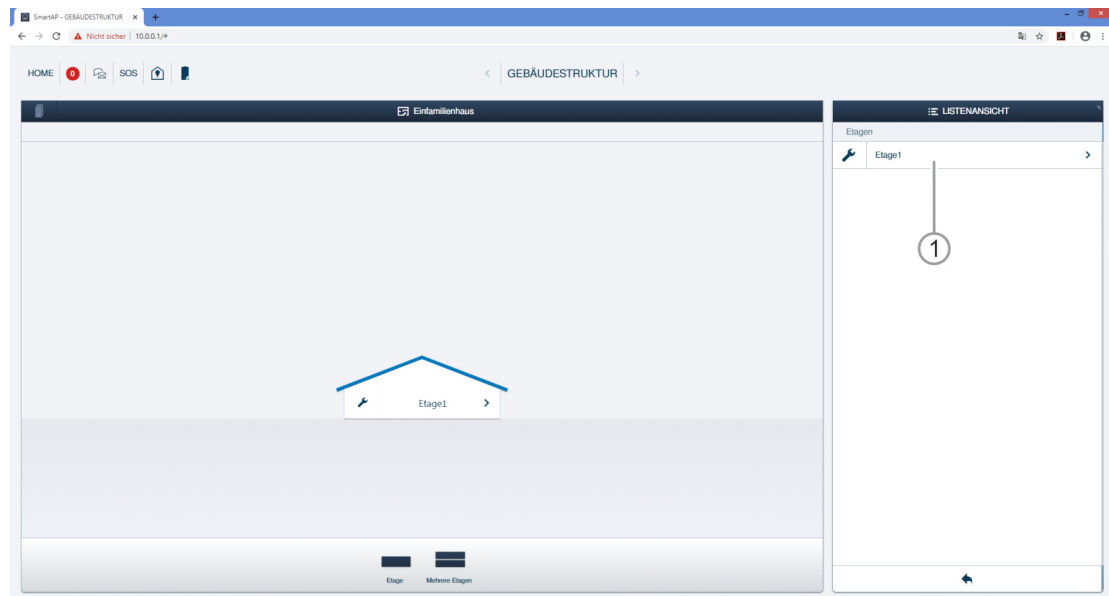


Abb. 88: Etage zur weiteren Bearbeitung auswählen.

5. Etage in der Liste [1] anklicken, um sie zur weiteren Bearbeitung auszuwählen.

5.3.3 Räume anlegen

Führen Sie zum Anlegen der Räume die folgenden Schritte durch:

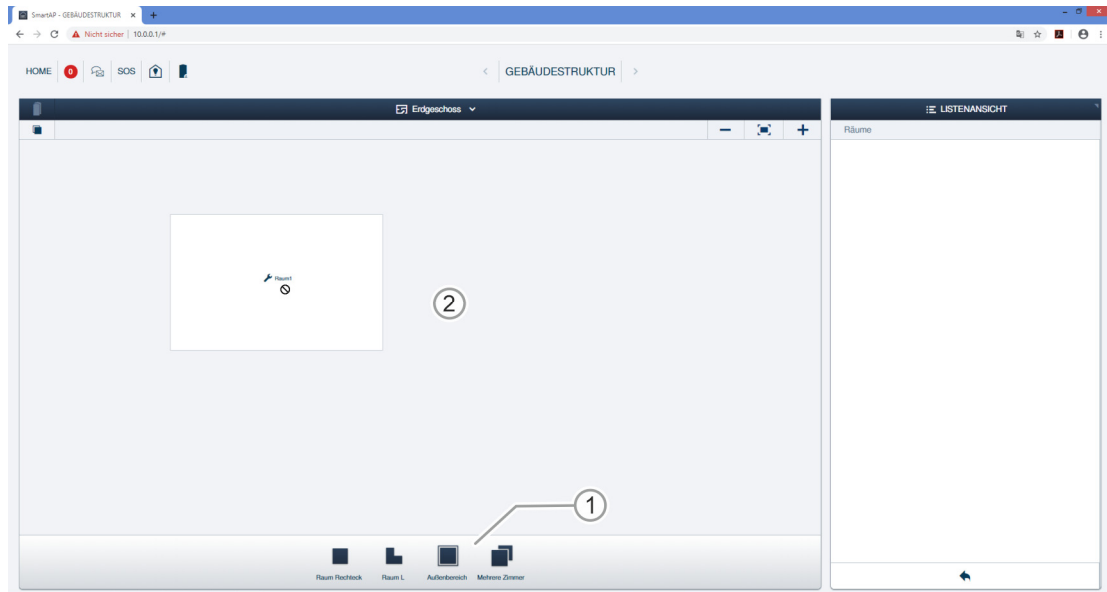


Abb. 89: Raumvariante wählen

1. Raumvariante aus der Liste [1] auswählen und auf die Arbeitsfläche [2] ziehen.

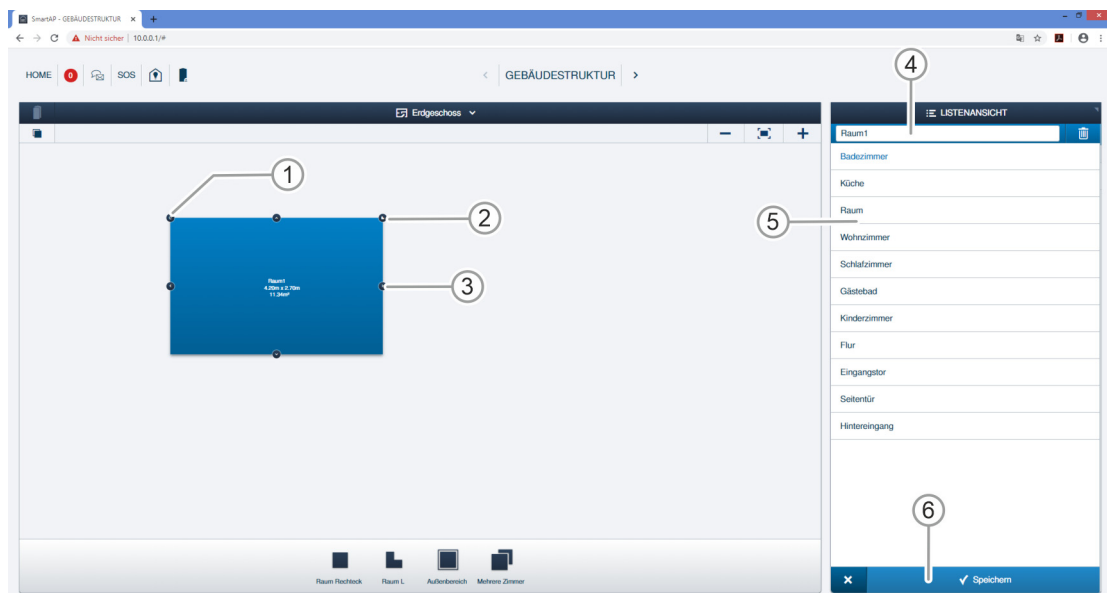


Abb. 90: Raum bearbeiten

2. Den Raum anklicken.
 - Der Raum wird blau hinterlegt. Am Rand des Raums erscheinen Schaltflächen, mit denen der Raum in Form und Größe verändert werden kann:
 - Mit Schaltfläche [1] wird der Raum gedreht.
 - Mit Schaltfläche [2] wird der Raum vergrößert oder verkleinert.
 - Mit Schaltfläche [3] wird die Position der einzelnen Kanten verändert.

3. Raumnamen im Feld [4] eintragen oder vorhandenen Raumnamen aus der Liste [5] auswählen.
4. Schaltfläche „Speichern“ [6] klicken.

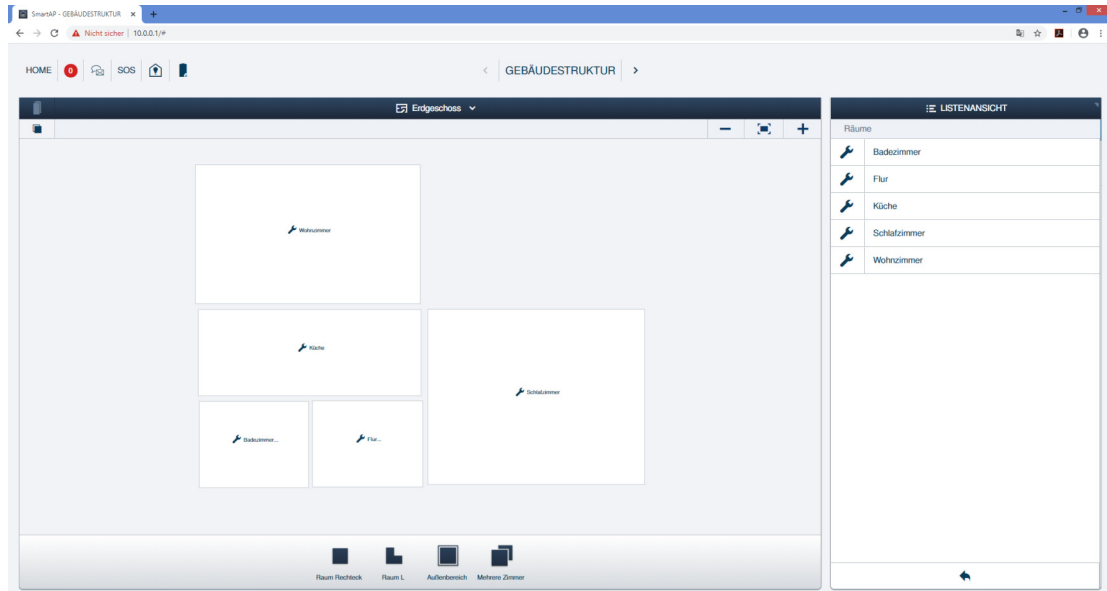


Abb. 91: Weitere Räume anlegen

5. Arbeitsschritte wiederholen, bis der Grundriss der Etage komplett erstellt ist.

5.4 Zutrittskontrolle

Im Menüpunkt „Zutrittskontrolle“ im Hauptmenü des „Smart Access Point Pro“ erfolgen die Verteilung der Geräte des Systems Busch-AccessControl auf die einzelnen Räume und Etagen in der Gebäudestruktur. Weiterhin das Koppeln der Geräte des Systems Busch-AccessControl.



Abb. 92: Menü "Zutrittskontrolle"

Im Menüpunkt „Zutrittskontrolle“ [1] werden die folgenden Einstellungen vorgenommen:

- Smart Access Point Pro hinzufügen
- Elektronischer Schließzylinder hinzufügen
- Elektronischer Schließzylinder mit Smart Access Point Pro koppeln.

5.4.1 „Smart Access Point Pro“ platzieren

Führen Sie zum Platzieren eines „Smart Access Point Pro“ die folgenden Schritte durch:

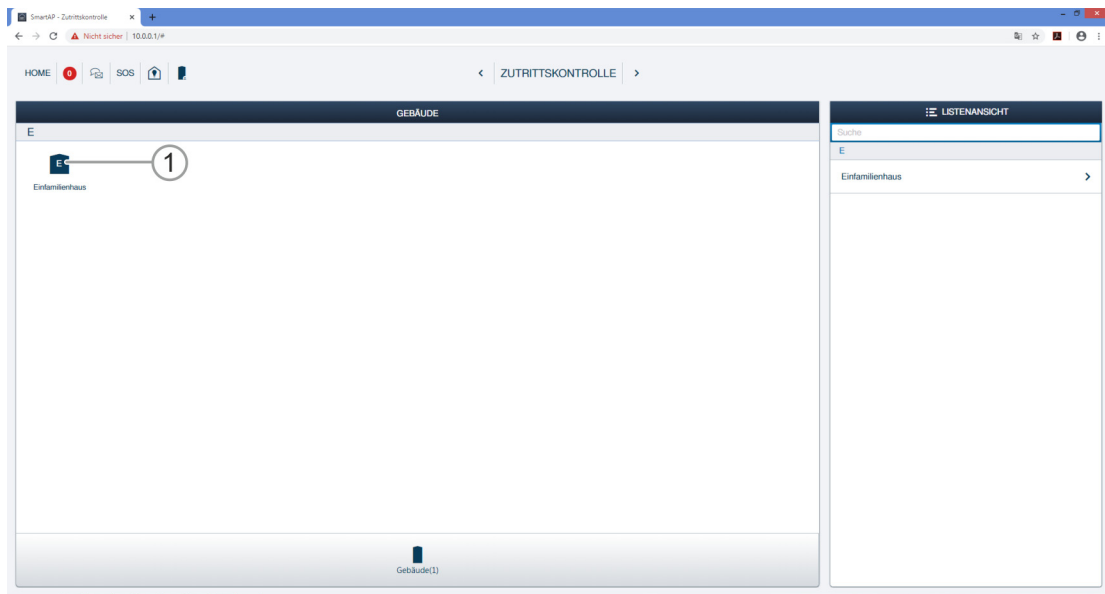


Abb. 93: Gebäude auswählen

1. Gewünschtes Gebäude [1] auswählen.

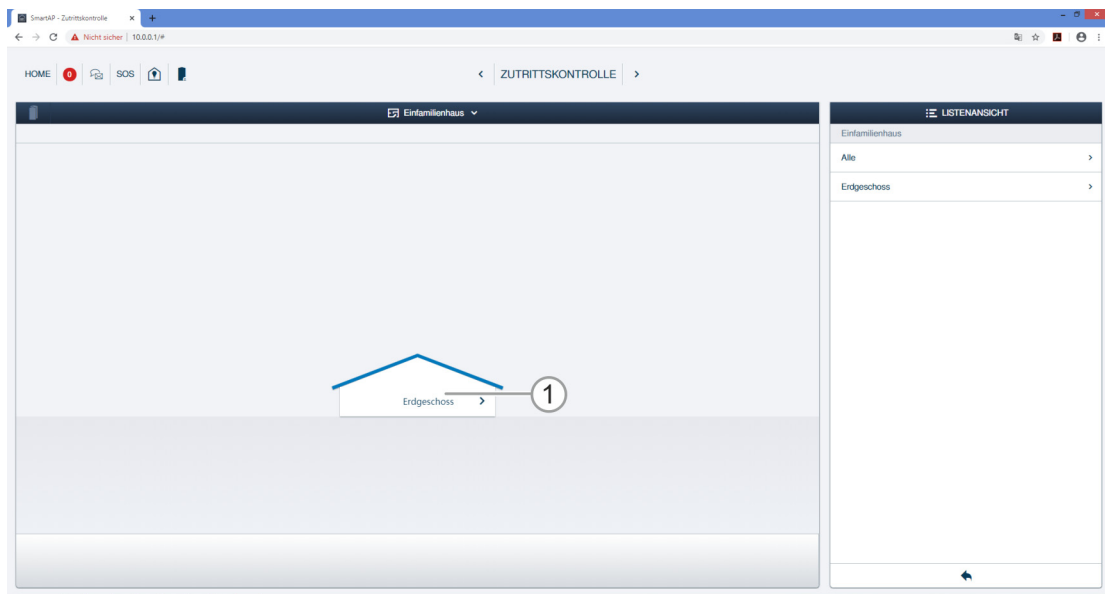


Abb. 94: Etage auswählen

2. Gewünschte Etage [1] auswählen.

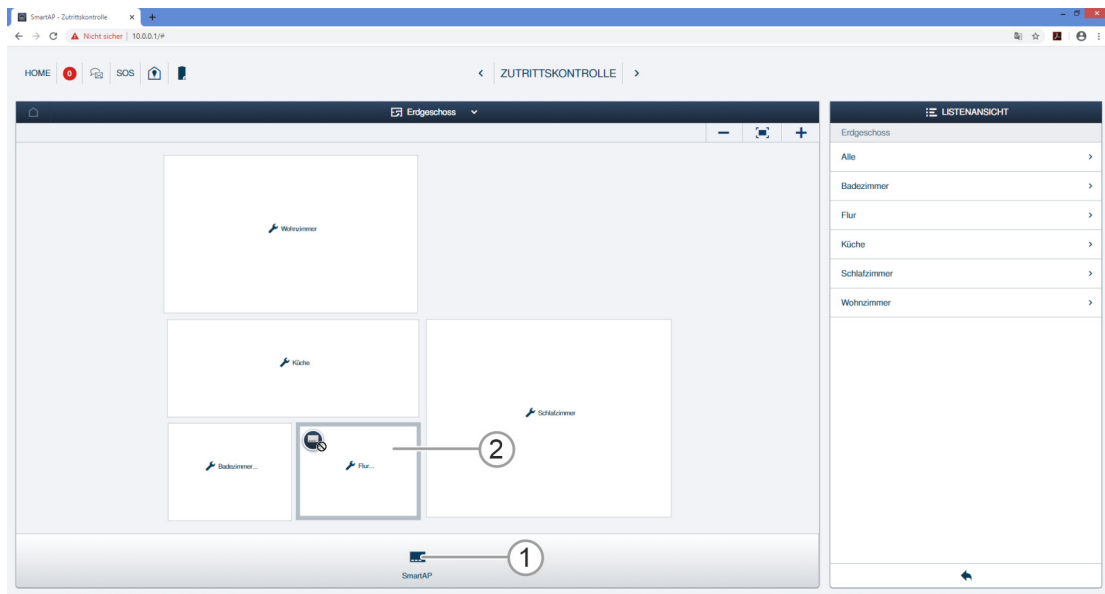


Abb. 95: „Smart Access Point Pro“ auf den Raum ziehen

3. „Smart Access Point Pro“ [1] auf den gewünschten Raum [2] ziehen.

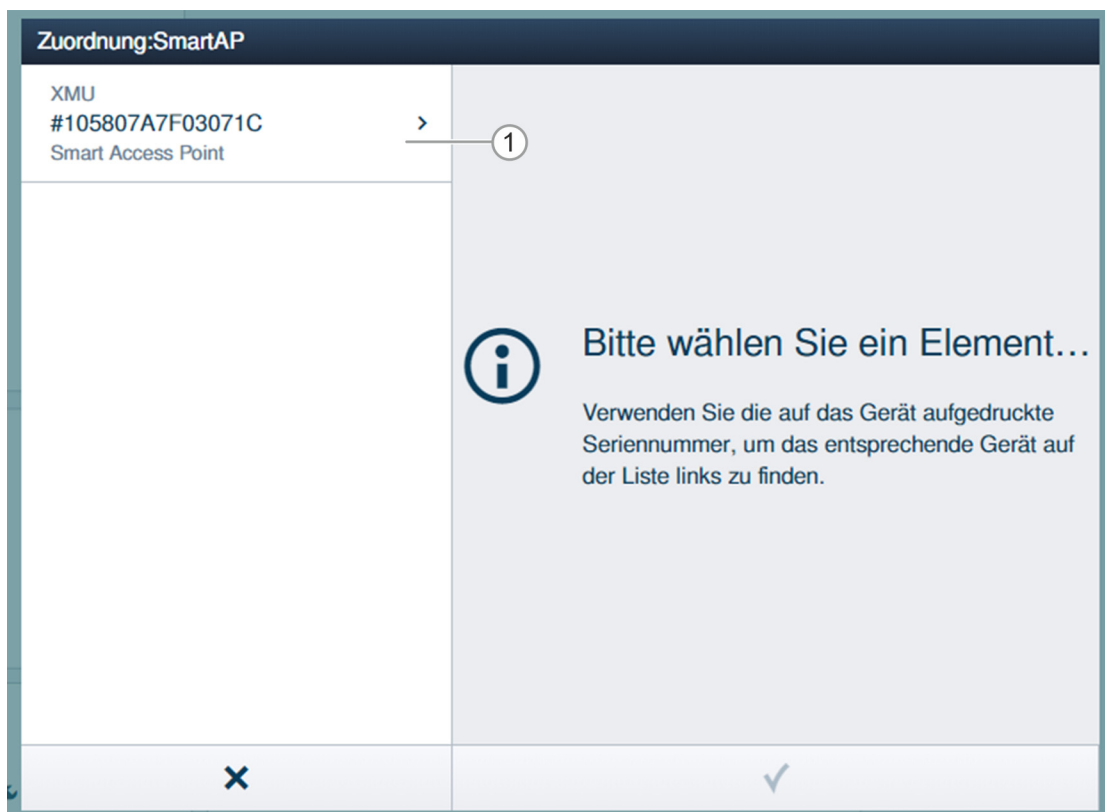


Abb. 96: Zuordnung „Smart Access Point Pro“

4. „Smart Access Point Pro“ aus der Liste [1] auswählen.

The screenshot shows a software interface for assigning a Smart Access Point. The title bar reads 'Zuordnung: SmartAP'. On the left, a card displays the device ID 'XMU #105807A7F03071C' and the label 'Smart Access Point'. The main area is titled 'Gerät' and contains the following details:

Gebäude	Einfamilienhaus
Etage	Erdgeschoss
Raum	Flur
Gerätename	Smart Access Point
Kurz-ID	XMU
Seriennummer	105807A7F03071C

Below the details, there is a 'Name' field containing the text 'Smart Access Point', which is marked with a circled '1'. At the bottom right, there is a checkmark icon marked with a circled '2'. The bottom left corner features a close button (X).

Abb. 97: Zuordnung „Smart Access Point Pro“ - Details

5. Gewünschte Bezeichnung für „Smart Access Point Pro“ in Feld [1] eingeben.
6. Schaltfläche „Speichern“ [2] klicken.

5.4.2 „RF/IP Gateway“ platzieren

Führen Sie zum Platzieren eines „RF/IP Gateway“ die folgenden Schritte durch:

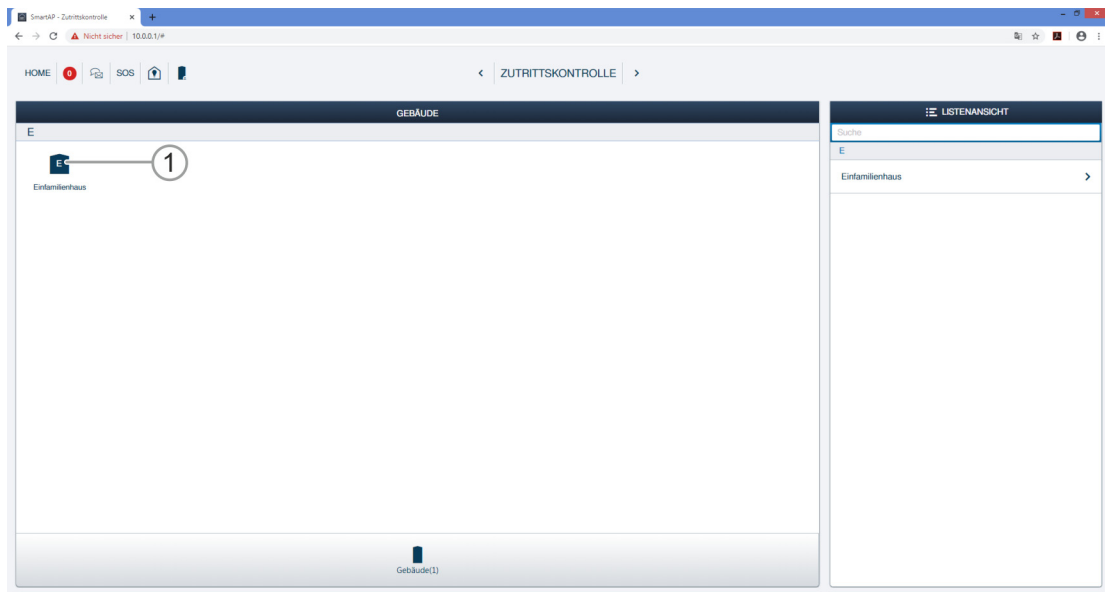


Abb. 98: Gebäude auswählen

1. Gewünschtes Gebäude [1] auswählen.

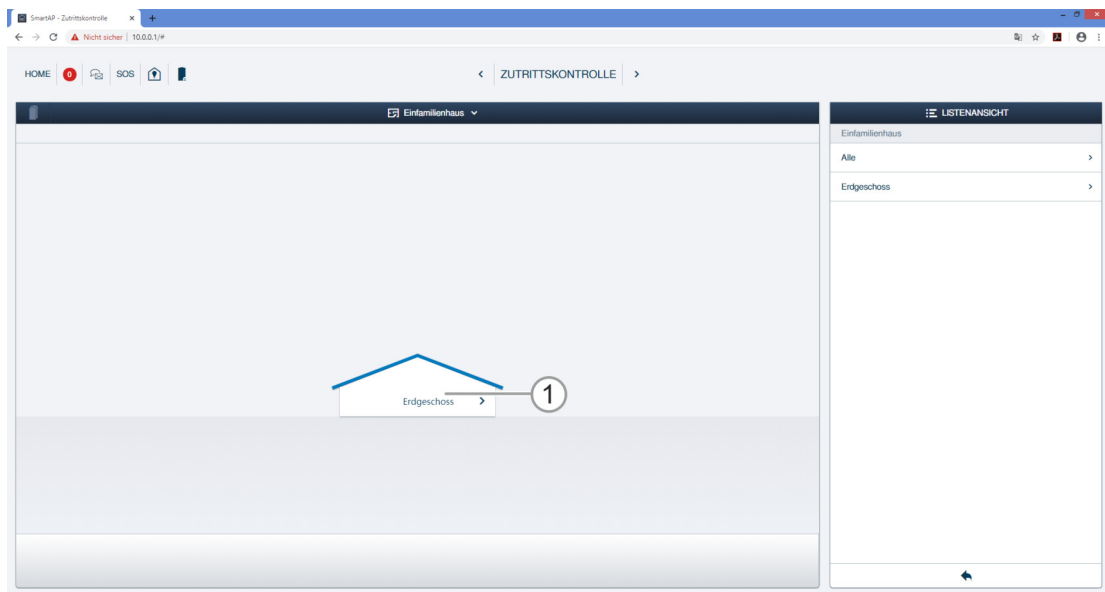


Abb. 99: Etage auswählen

2. Gewünschte Etage [1] auswählen.

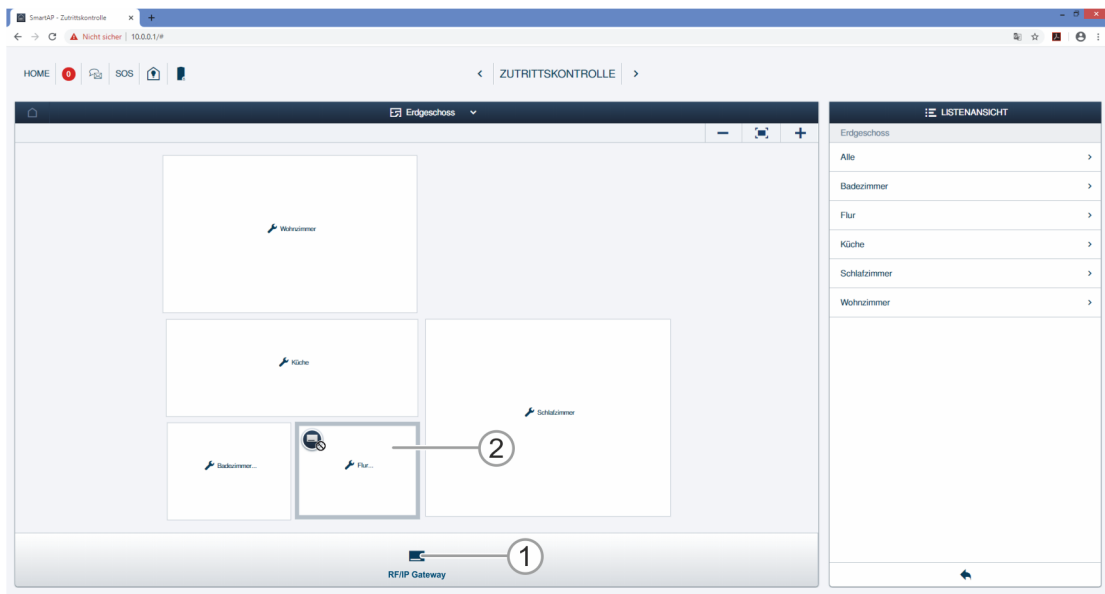


Abb. 100: „RF/IP Gateway“ auf den Raum ziehen

3. „RF/IP Gateway“ [1] auf den gewünschten Raum [2] ziehen.



Abb. 101: Zuordnung „RF/IP Gateway“

4. „RF/IP Gateway“ aus der Liste [1] auswählen.

Zuordnung: RF/IP Gateway

XMU
#105807A7F03071C
RF/IP Gateway

Gerät

Gebäude: Einfamilienhaus
Etage: Erdgeschoss
Raum: Flur
GeräteName: RF/IP Gateway

Kurz-ID: XMU
Seriennummer: 105807A7F03071C

Name: RF/IP Gateway (1)

(2)

Abb. 102: Zuordnung „RF/IP Gateway“ - Details

5. Gewünschte Bezeichnung für „RF/IP Gateway“ in Feld [1] eingeben.
6. Schaltfläche „Speichern“ [2] klicken.

5.4.3 „Elektronischer Schließzylinder“ platzieren

Führen Sie zum Platzieren eines „Elektronischer Schließzylinder“ die folgenden Schritte durch:

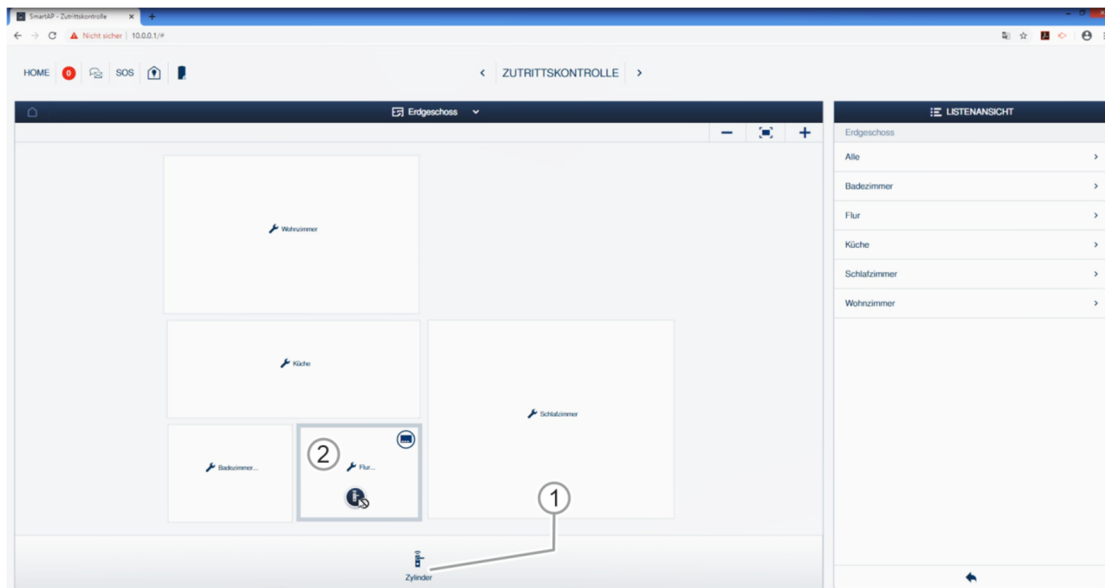


Abb. 103: „Elektronischer Schließzylinder“ auf Raum ziehen

1. „Elektronischer Schließzylinder“ aus der Liste [1] auf den gewünschten Raum [2] ziehen.



Abb. 104: Zuordnung des „Elektronischer Schließzylinder“ 1.

2. „Elektronischer Schließzylinder“ aus der Liste auswählen.

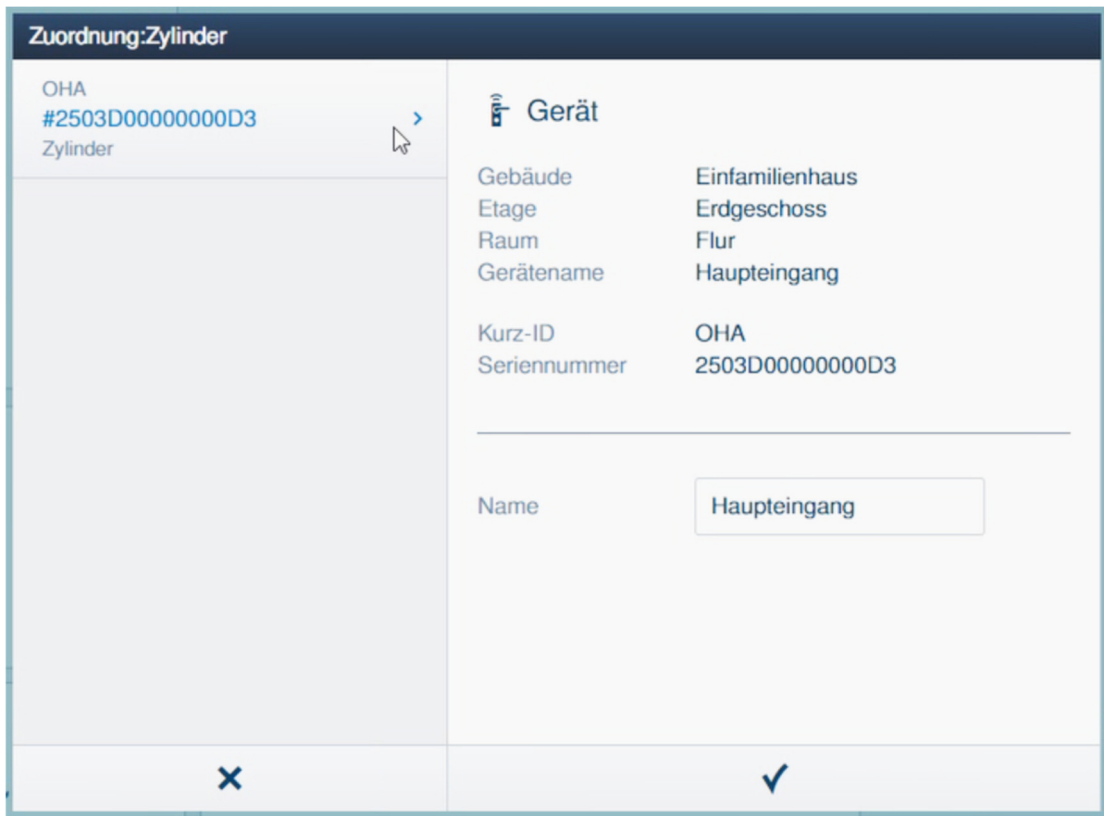


Abb. 105: Zuordnung des „Elektronischer Schließzylinder“ 2.

3. Einen Namen für den „Elektronischer Schließzylinder“ eingeben und Schaltfläche „Speichern“ klicken.

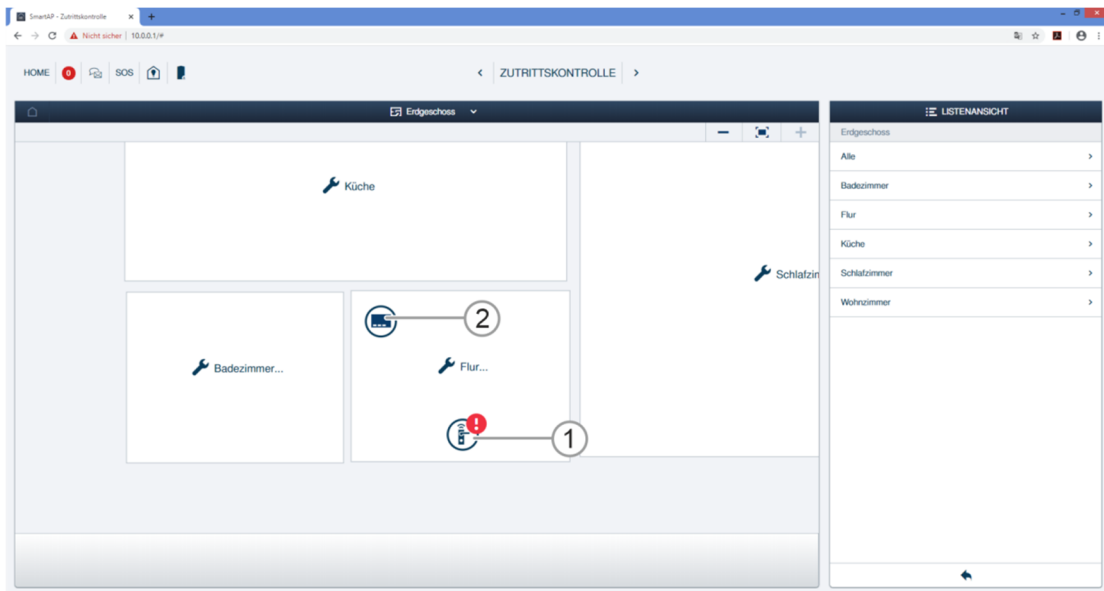


Abb. 106: „Elektronischer Schließzylinder“ im Raum

Der neu angelegte „Elektronischer Schließzylinder“ [1] und der „Smart Access Point Pro“ [2] werden im Raum angezeigt.

Das Symbol „!“ und die fehlende Verbindungslinie zeigen, dass es noch keine Verbindung zwischen den beiden Geräten gibt.

5.4.4 Elektronischer Schließzylinder mit Smart Access Point koppeln

Der neu angelegte „Elektronischer Schließzylinder“ muss nun mit dem nächstgelegenen „Smart Access Point Pro“ verknüpft werden.

Führen Sie zum Koppeln des „Elektronischer Schließzylinder“ mit dem „Smart Access Point Pro“ die folgenden Schritte durch:

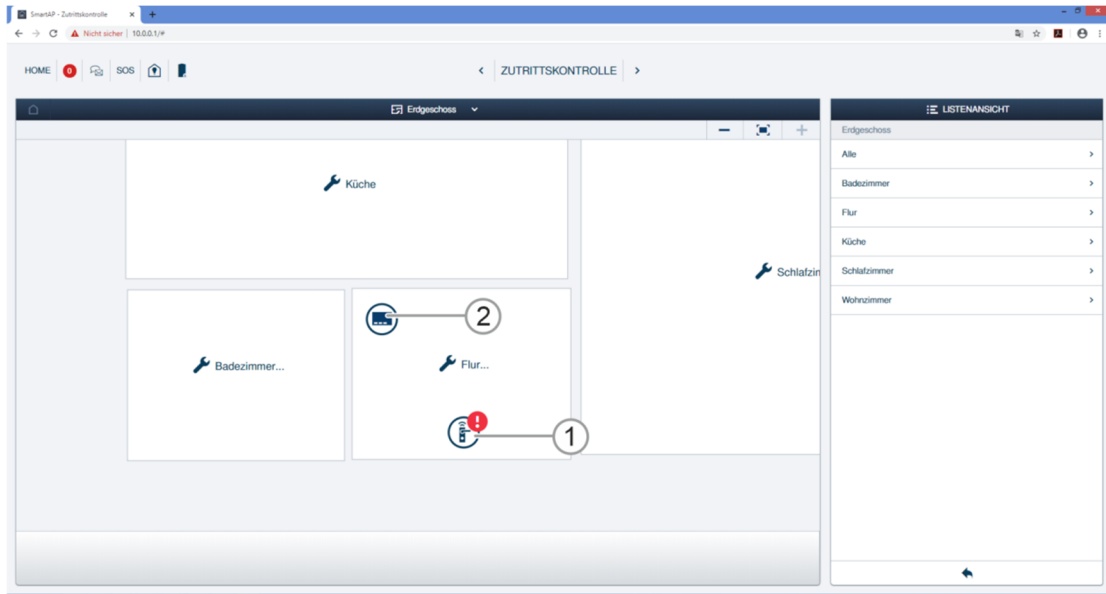


Abb. 107: „Elektronischer Schließzylinder“ mit „Smart Access Point Pro“ koppeln

1. Auf den „Elektronischer Schließzylinder“ [1] klicken.
2. Auf den „Smart Access Point Pro“ [2] klicken



Abb. 108: Kopplungsvorgang 1/3

3. Anweisungen auf dem Display folgen und **Wartungskarte** vor den „Elektronischer Schließzylinder“ halten.

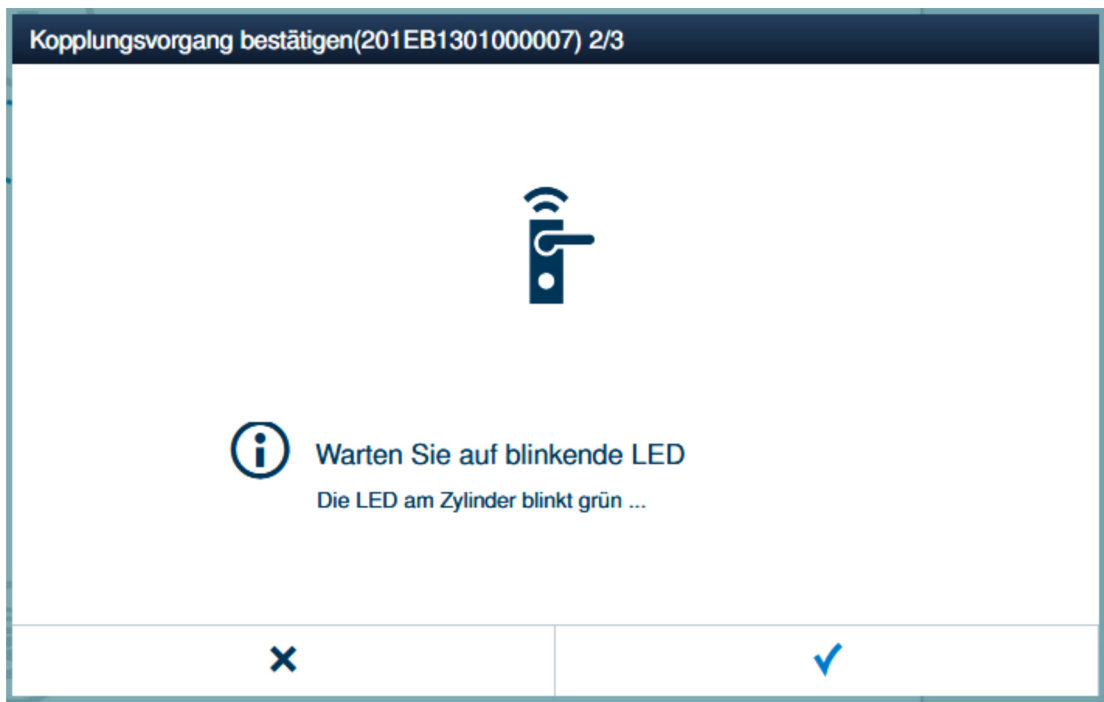


Abb. 109: Kopplungsvorgang 2/3

4. **Wartungskarte** so lange vor den „Elektronischer Schließzylinder“ halten, bis die LED grün blinkt.



Abb. 110: Kopplungsvorgang 3/3

Der „Elektronischer Schließzylinder“ ist nun mit dem „Smart Access Point Pro“ gekoppelt.

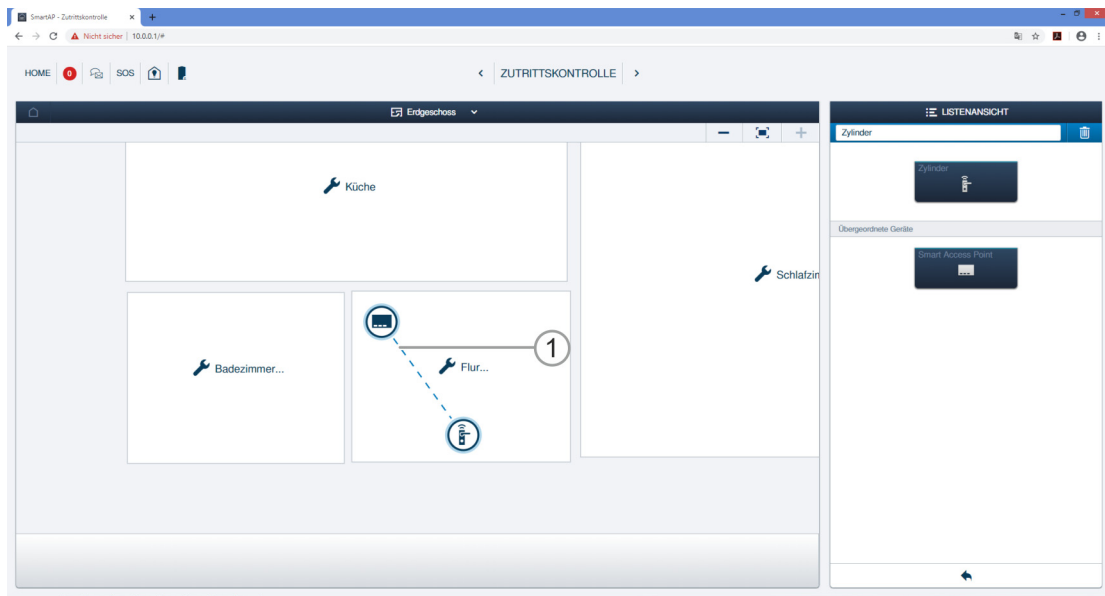


Abb. 111: „Elektronischer Schließzylinder“ angelegt

Die **Verbindung** zwischen beiden Geräten wird durch eine gestrichelte Linie [1] angezeigt.

Der „Elektronischer Schließzylinder“ ist betriebsbereit und kann über die Benutzerverwaltung mit Schließrechten belegt werden (siehe Kapitel 5.5 „Benutzerverwaltung“ auf Seite 118).

5.4.5 Repeater platzieren



5.4.6 Repeater koppeln

Führen Sie zum Koppeln des Repeaters mit dem „Smart Access Point Pro“ die folgenden Schritte durch:

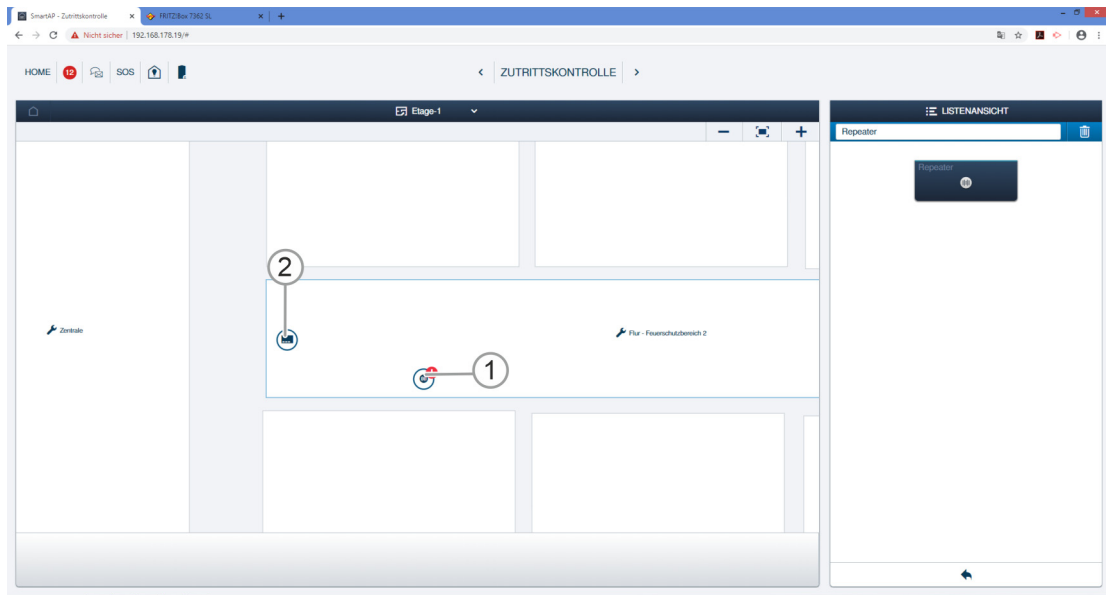


Abb. 112: Repeater mit „Smart Access Point Pro“ koppeln

1. Repeater[1] aus der Liste in den gewünschten Raum ziehen.
2. Auf den Repeater [1] klicken.
3. Auf den „Smart Access Point Pro“ [2] klicken.

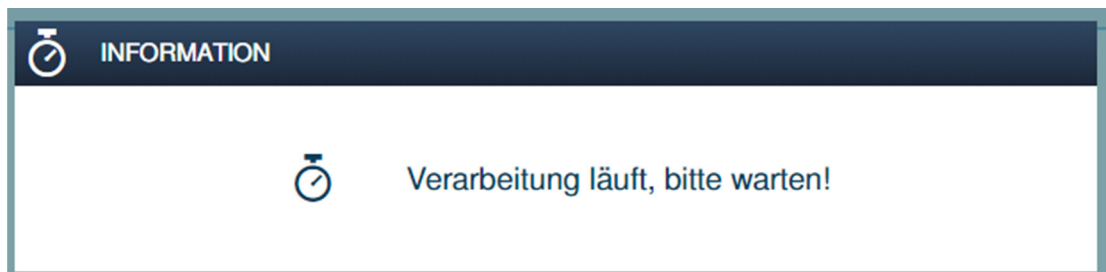


Abb. 113: Kopplungsvorgang

- Der Fortschritt des Kopplungsvorgangs wird im Fenster angezeigt

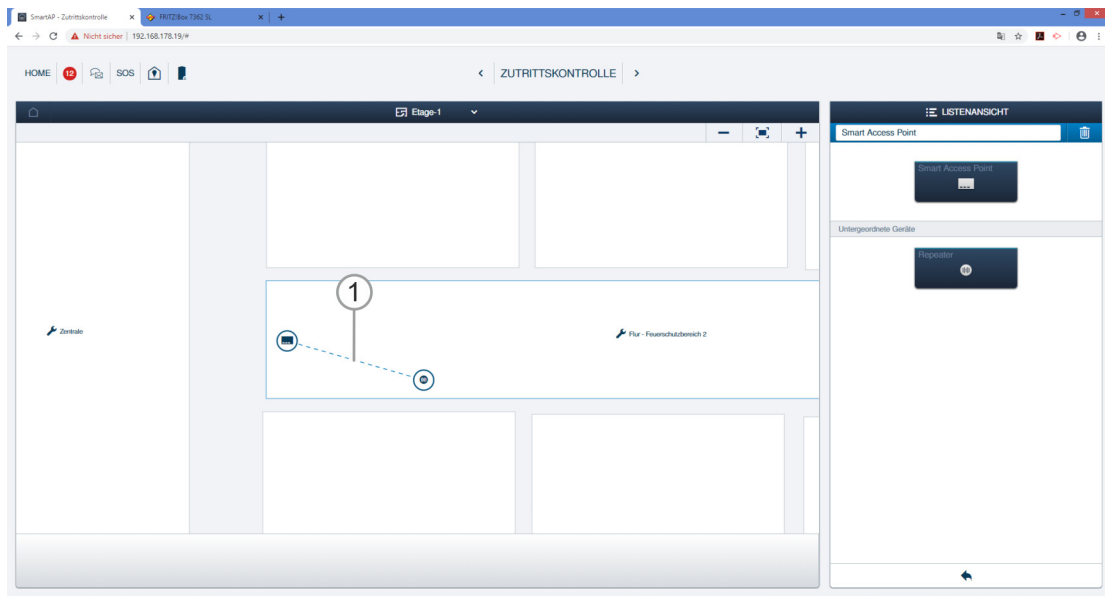


Abb. 114: Repeater mit „Smart Access Point Pro“ gekoppelt

- Der Repeater ist nun mit dem „Smart Access Point Pro“ gekoppelt. Die **Verbindung** zwischen beiden Geräten wird durch eine gestrichelte Linie [1] angezeigt.

5.5 Benutzerverwaltung

Die Verwaltung der Schließzylinder, Transponderschlüssel und Schließberechtigungen erfolgt über den Menüpunkt „Benutzerverwaltung“ im Hauptmenü des „Smart Access Point Pro“.

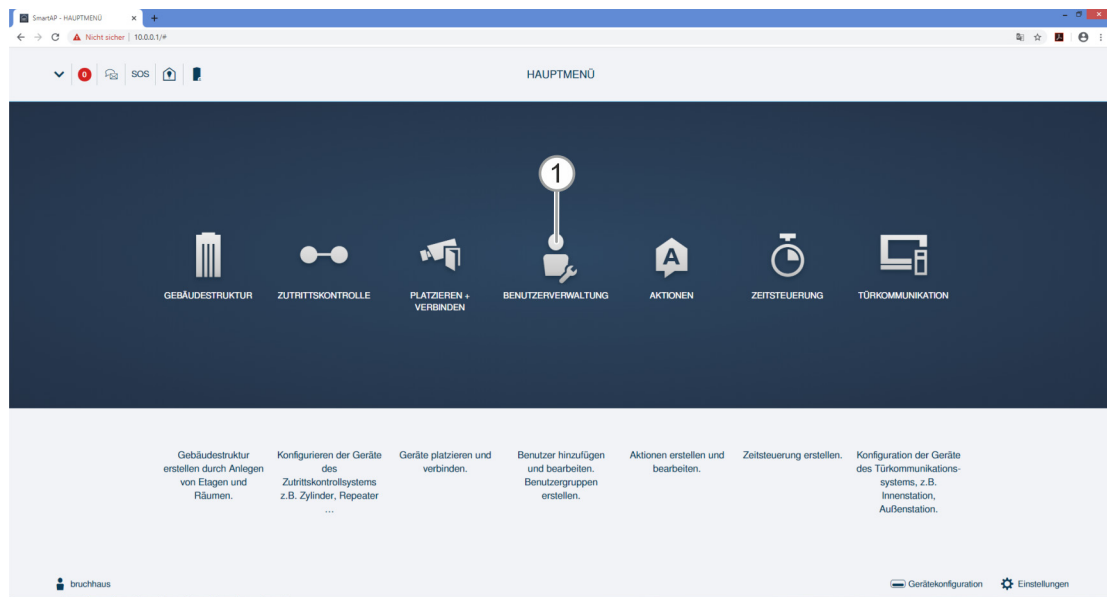


Abb. 115: Menüpunkt „Benutzerverwaltung“

Im Menüpunkt „Benutzerverwaltung“ [1] werden die folgenden Einstellungen vorgenommen:

- Neue Benutzer anlegen.
- Neue Benutzergruppen anlegen.
- Transponderschlüssel anlegen.
- Transponderschlüssel einem Benutzer zuweisen (Authentifizierung).
- Schließberechtigungen für Benutzer und Transponderschlüssel einstellen und verwalten.

Zum Vergabe von Schließrechten sind die folgenden Schritte notwendig:

- Benutzer anlegen, siehe Kapitel 5.5.1 „Benutzer anlegen“ auf Seite 119.
- Transponderschlüssel an einem „Elektronischer Schließzylinder“ einlernen (Authentifizierung) siehe Kapitel 5.5.2 „Authentifizierung hinzufügen“ auf Seite 120
- Benutzer das Schließrecht zu einem „Elektronischer Schließzylinder“ erteilen, siehe Kapitel 5.5.3 „Schließrecht erteilen“ auf Seite 125.

5.5.1 Benutzer anlegen

Führen Sie zum Hinzufügen eines Benutzers die folgenden Schritte durch:

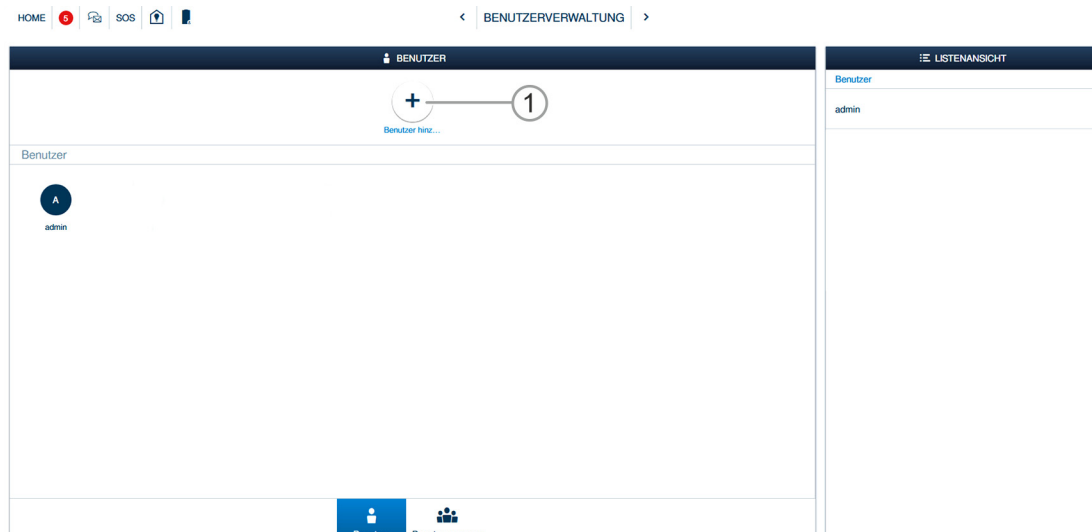


Abb. 116: Benutzer hinzufügen

1. Auf die Schaltfläche „Benutzer hinzufügen“ [1] klicken.



Abb. 117: Benutzerdaten eingeben

2. Den Namen des Benutzers im Feld [1] eingeben.
3. Die Daten (z.B. Passwort, E-Mailadresse und Benutzerrolle) in den Parameterfeldern eintragen.



Hinweis

Die genauen Beschreibungen der sichtbaren Benutzerparameter befinden sich in den Systemhandbüchern der entsprechenden Geräte.

5.5.2 Authentifizierung hinzufügen

Der Begriff „Authentifizierung“ umfasst alle im System vorhandenen Transponderschlüssel und deren Zuordnung zu den angelegten Benutzern / Benutzergruppen und „Elektronischer Schließzylinder“.

Für jeden Transponderschlüssel, der eine Schließberechtigung erhalten soll, muss eine Authentifizierung im „Smart Access Point Pro“ angelegt werden.

Führen Sie zum Hinzufügen einer Authentifizierung die folgenden Schritte durch:

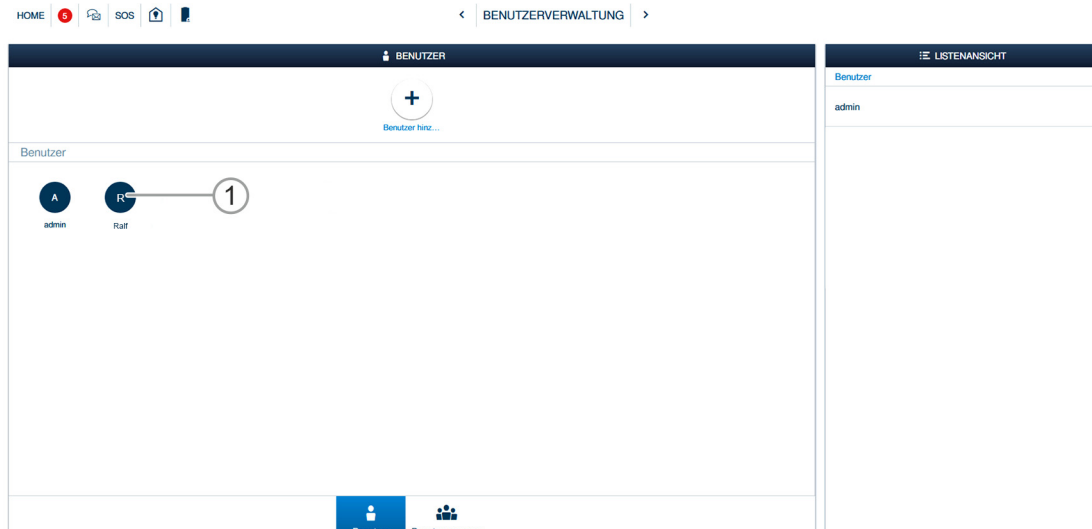


Abb. 118: Benutzer auswählen.

1. Den gewünschten Benutzer [1] für den neuen Transponderschlüssel auswählen.

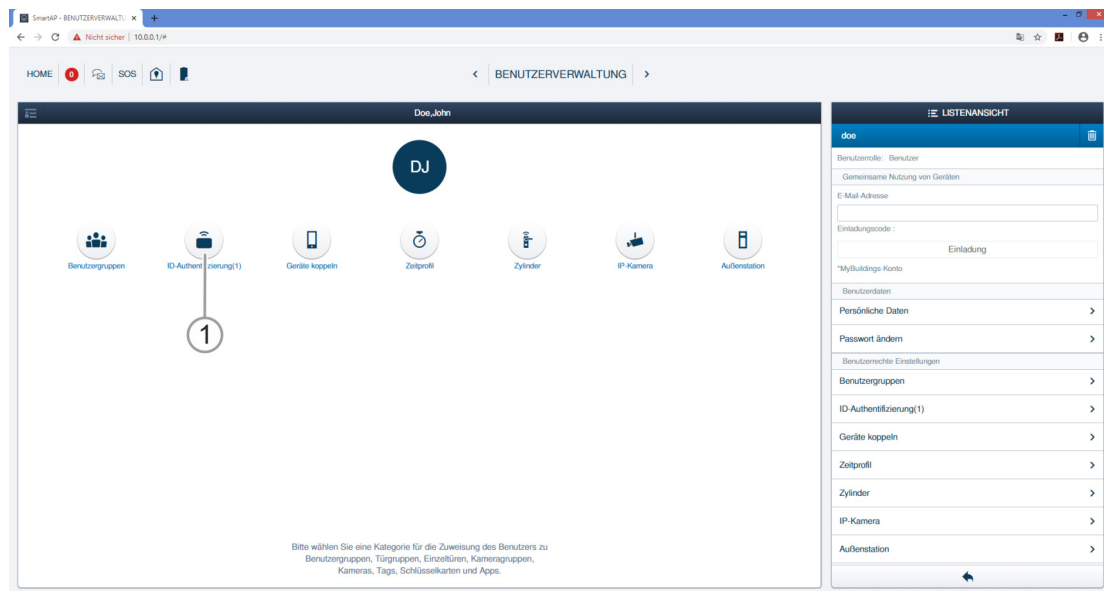


Abb. 119: ID-Authentifizierung auswählen

2. Schaltfläche „ID-Authentifizierung“ [1] klicken.

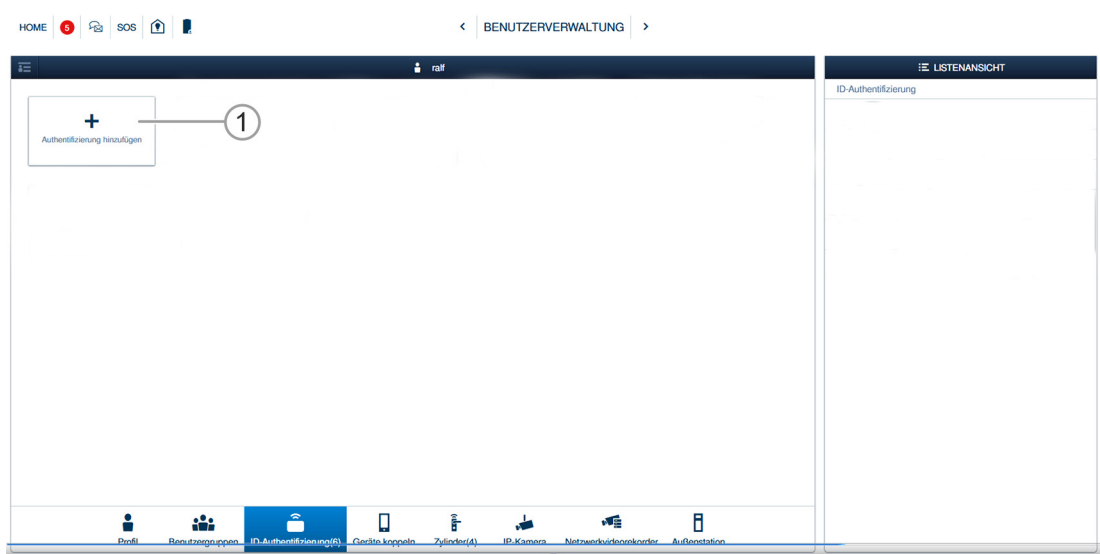


Abb. 120: Authentifizierung hinzufügen

3. Schaltfläche „Authentifizierung hinzufügen“ [1] klicken.



Abb. 121: Schaltfläche „Authentifizierung hinzufügen für Zutrittskontrolle“

4. Schaltfläche „Authentifizierung hinzufügen für Zutrittskontrolle“ [1] klicken.



Abb. 122: Neue Authentifizierung

5. Im Feld „Kartenname“ [1] einen eindeutig identifizierbaren Namen für den neuen Transponderschlüssel eingeben.

AUTHENTIFIZIERUNG HINZUFÜGEN

Neue Authentifizierung

Kartename: weißer Tag 4 ...041

Kartentyp: rfid

Gültigkeitszeit...: Unbegrenzte Gültigkeit

Kartenlesegerät: Select reader

Kartennummer: RF-Zylinder KI EU1
RF-Zylinder KI MOR1
RF-Zylinder KI CH2
RF-Zylinder KI RIM

Abb. 123: „Elektronischer Schließzylinder“ auswählen

6. Im Feld „Kartenlesegerät“ [2] den ersten gewünschten „Elektronischer Schließzylinder“ auswählen, zu dem der Transponderschlüssel Schließberechtigungen erhalten soll.

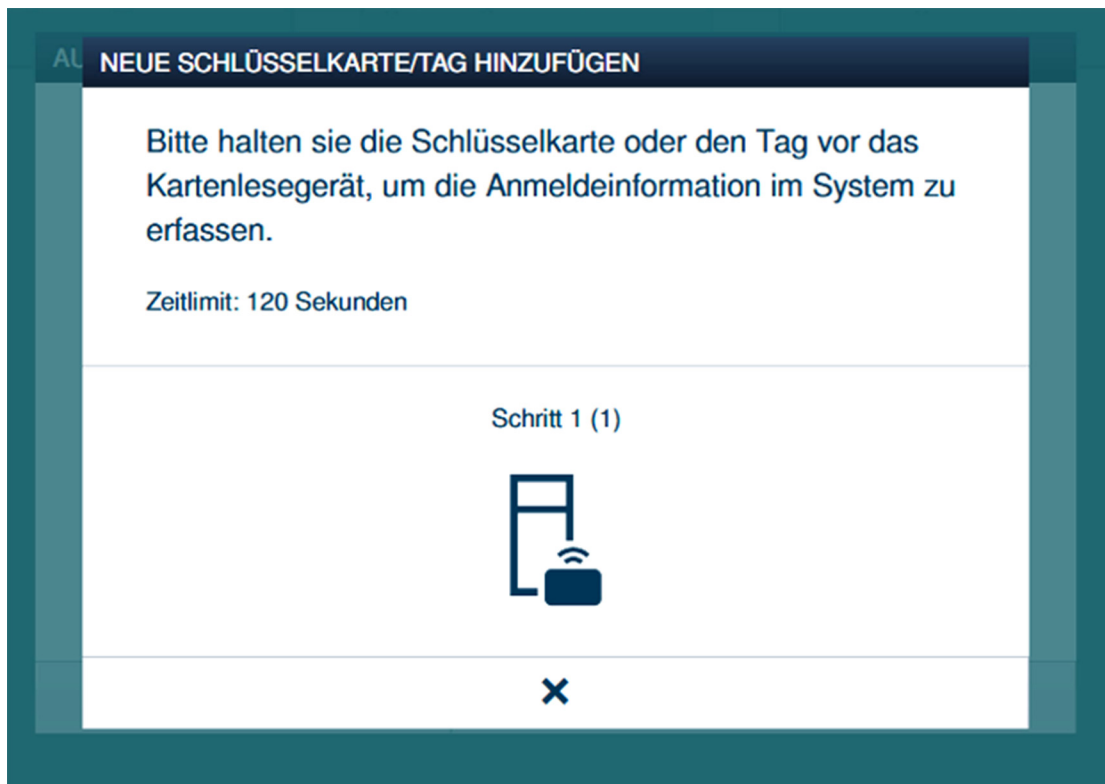


Abb. 124: Transponderschlüssel vorhalten

7. Den Anweisungen auf dem Display folgen und den Transponderschlüssel vor den ausgewählten „Elektronischer Schließzylinder“ halten.
 - Die Kartenummer des Transponderschlüssels wird automatisch eingetragen.
 - Der Transponderschlüssel ist nun auf den ausgewählten „Elektronischer Schließzylinder“ angelernt.



Hinweis

Anschließend muss dem Benutzer und seinem Transponderschlüssel noch das Schließrecht zu den gewünschten „Elektronischer Schließzylinder“ zugewiesen werden.

5.5.3 Schließrecht erteilen

Alle angelegten Schließzylinder werden im Bereich „nicht zugewiesen“ [1] angezeigt.
Der Benutzer hat noch kein Schließrecht. Das Schließrecht muss ihm nun zugewiesen werden.

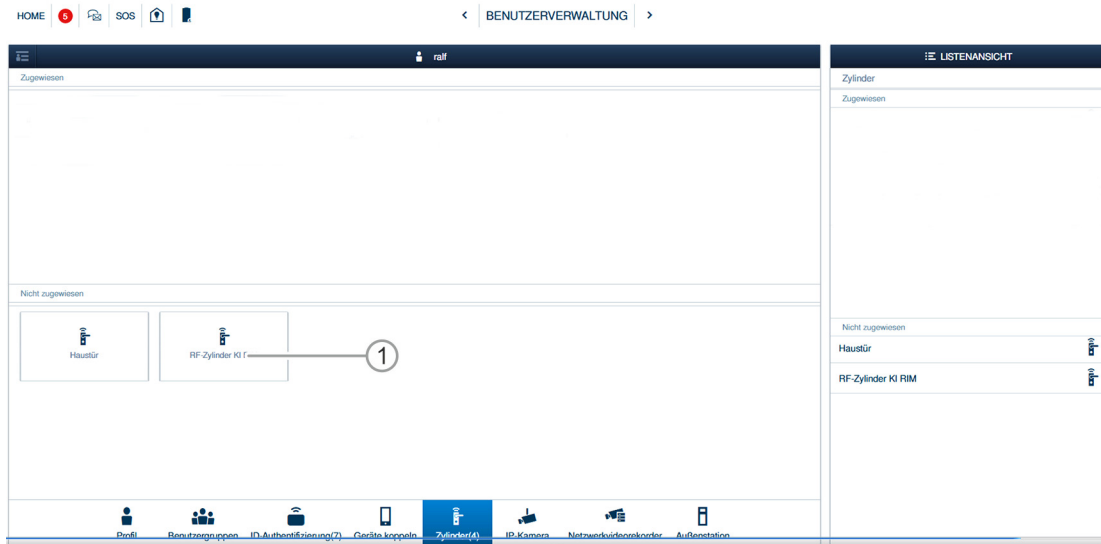


Abb. 125: „Elektronischer Schließzylinder“ nicht zugewiesen

Um dem Benutzer das Schließrecht für den gewünschten „Elektronischer Schließzylinder“ zu erteilen, führen Sie die folgenden Schritte durch:

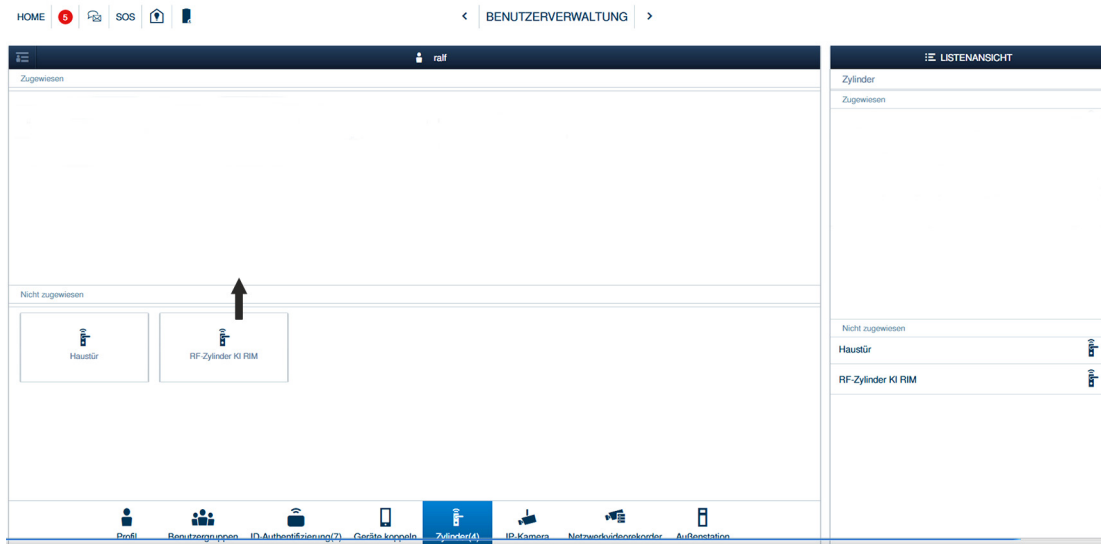


Abb. 126: Schließrecht für „Elektronischer Schließzylinder“ zuweisen

1. Den „Elektronischer Schließzylinder“ per Drag&Drop in die Fläche „Zugewiesen“ ziehen.

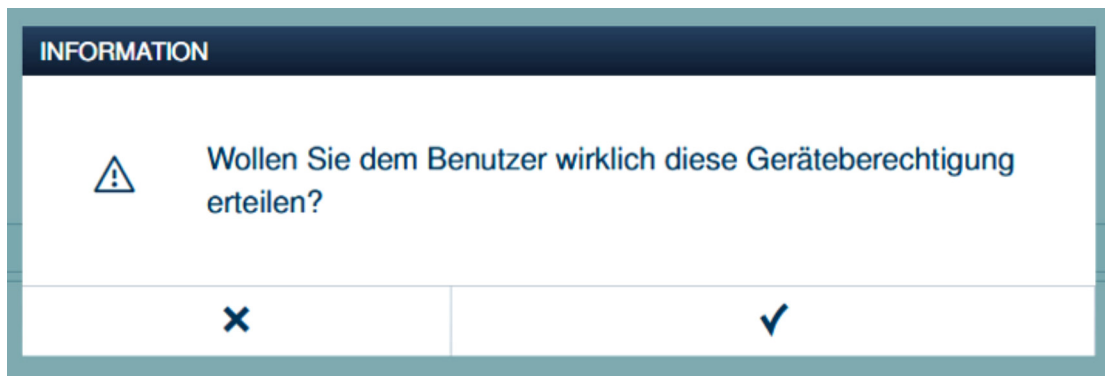


Abb. 127: Fenster „Geräteberechtigung“

2. Frage im Fenster „Geräteberechtigung“ bestätigen.

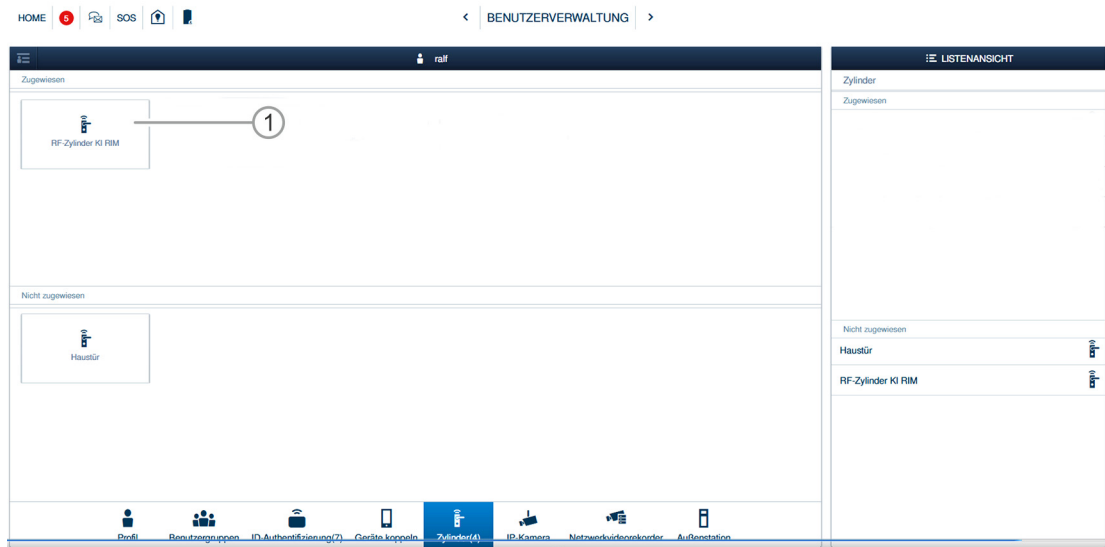


Abb. 128: „Elektronischer Schließzylinder“ zugewiesen

Der „Elektronischer Schließzylinder“ wird im Feld „Zugewiesen“ [1] angezeigt.

- Der Benutzer hat mit seinem Transponderschlüssel das Schließrecht zu diesem „Elektronischer Schließzylinder“.



Hinweis

Wurden dem Benutzer mehrere Transponderschlüssel zugewiesen, haben automatisch alle Transponderschlüssel das Schließrecht zu den „Elektronischer Schließzylinder“, die im Feld „Zugewiesen“ angezeigt werden.



Hinweis

Soll der Benutzer mit seinem Transponderschlüssel das Schließrecht zu mehreren „Elektronischer Schließzylinder“ erhalten, die Schritte 1 und 2 dieses Kapitels wiederholen, bis alle gewünschten „Elektronischer Schließzylinder“ im Feld „Zugewiesen“ aufgeführt sind.

5.6 Daten aus dem Menü "Benutzerverwaltung" löschen

Das Löschen der Schließzylinder, Transponderschlüssel und Schließberechtigungen erfolgt über den Menüpunkt „Benutzerverwaltung“ [1] im Hauptmenü des „Smart Access Point Pro“.

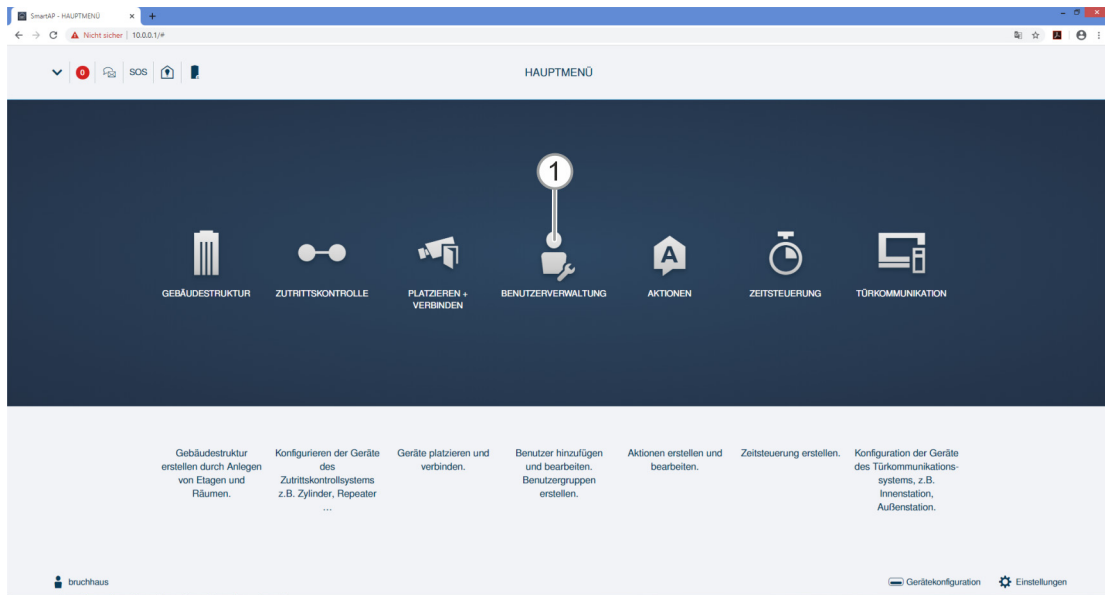


Abb. 129: Menüpunkt „Benutzerverwaltung“

5.6.1 Schließrecht löschen

Führen Sie zum Löschen eines Schließrechts die folgenden Schritte durch:

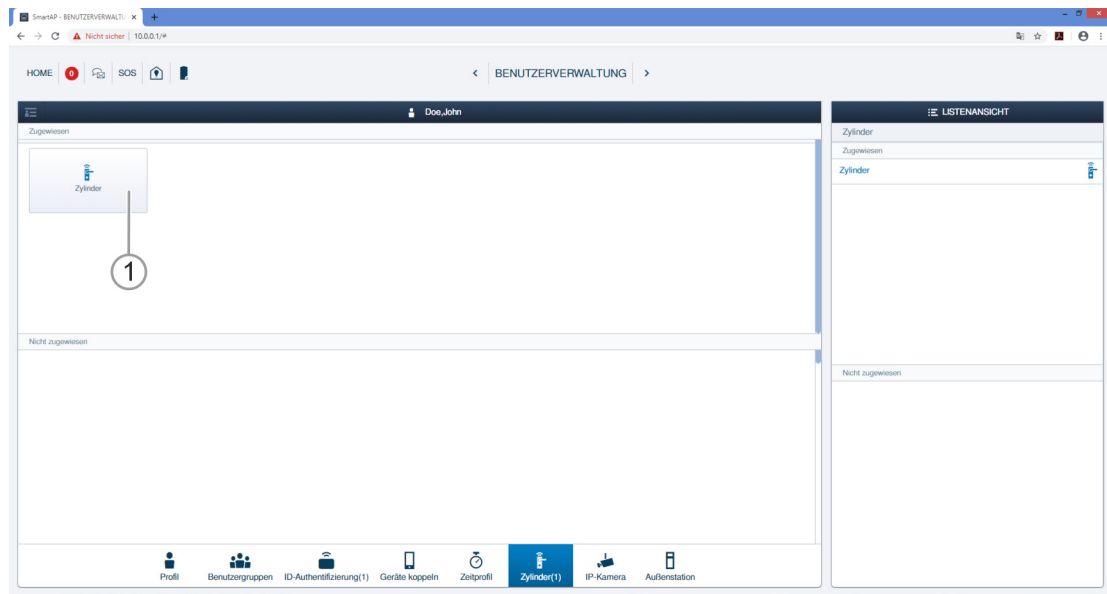


Abb. 130: „Elektronischer Schließzylinder“ zugewiesen

1. Auf den gewünschten Schließzylinder [1] klicken.

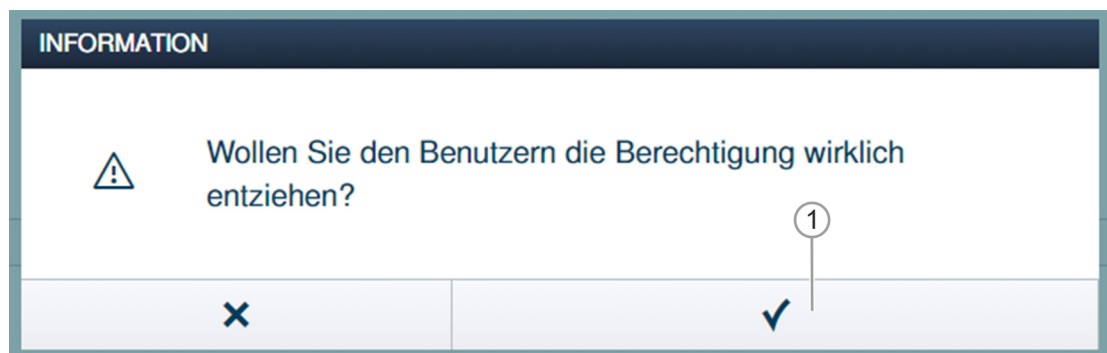


Abb. 131: Bestätigung Schließrecht entziehen

2. Frage mit der Schaltfläche [1] bestätigen.
 - Das Schließrecht für diesen Schließzylinder ist entzogen.

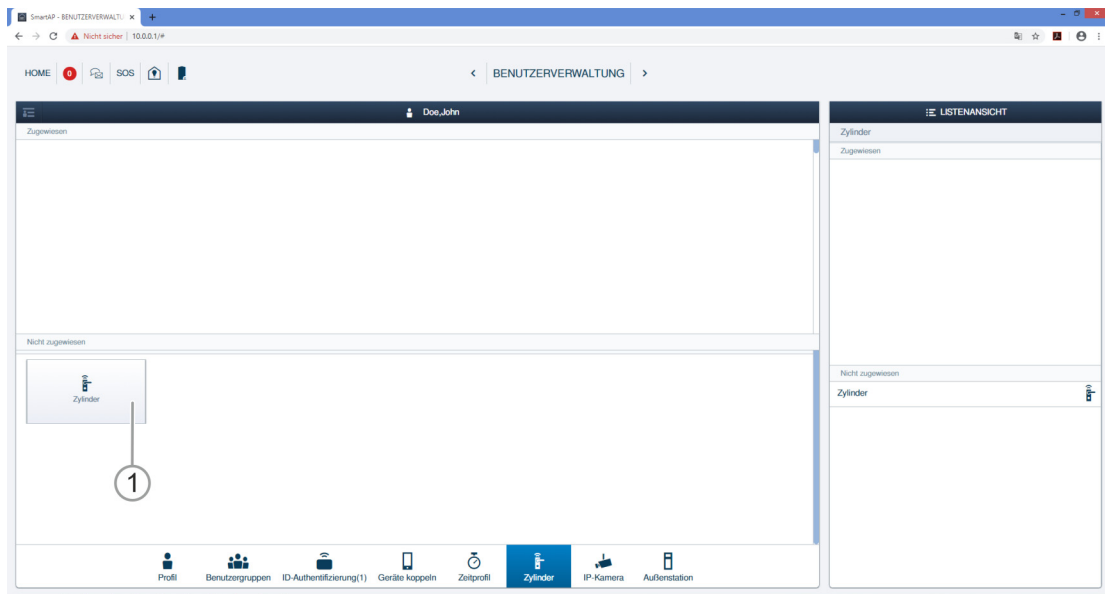


Abb. 132: „Elektronischer Schließzylinder“ nicht zugewiesen

Der Zylinder wird im Bereich „nicht zugewiesen“ [1] angezeigt.

5.6.2 Authentifizierung löschen

Führen Sie zum Löschen einer Authentifizierung (= eines Transponderschlüssels) die folgenden Schritte durch:

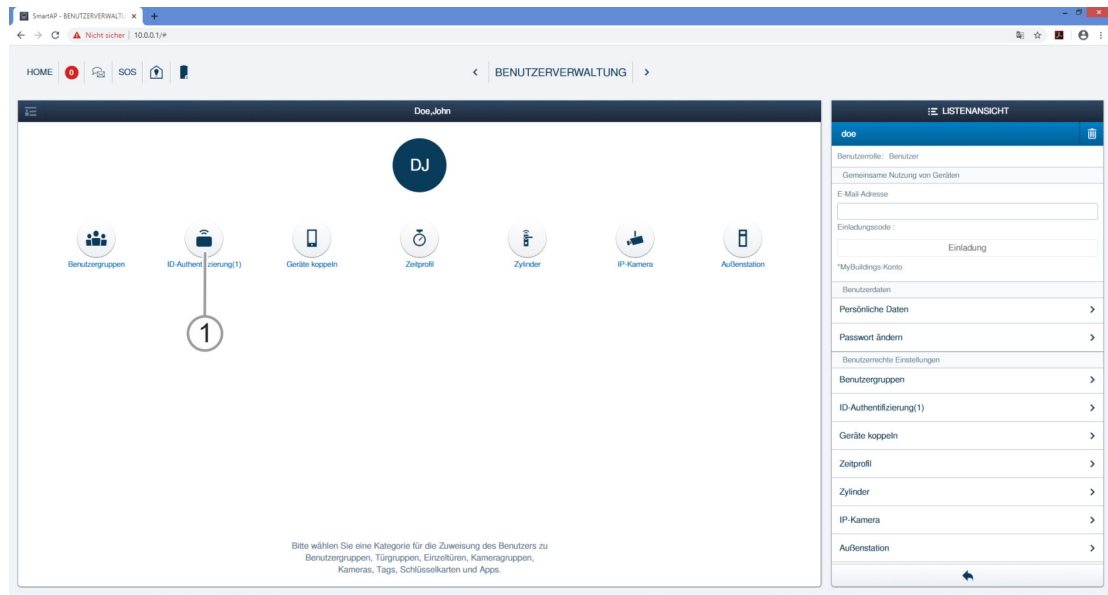


Abb. 133: ID-Authentifizierung

1. Schaltfläche „ID-Authentifizierung“ [1] anklicken.
 - Alle Authentifizierungen des Benutzers werden angezeigt.

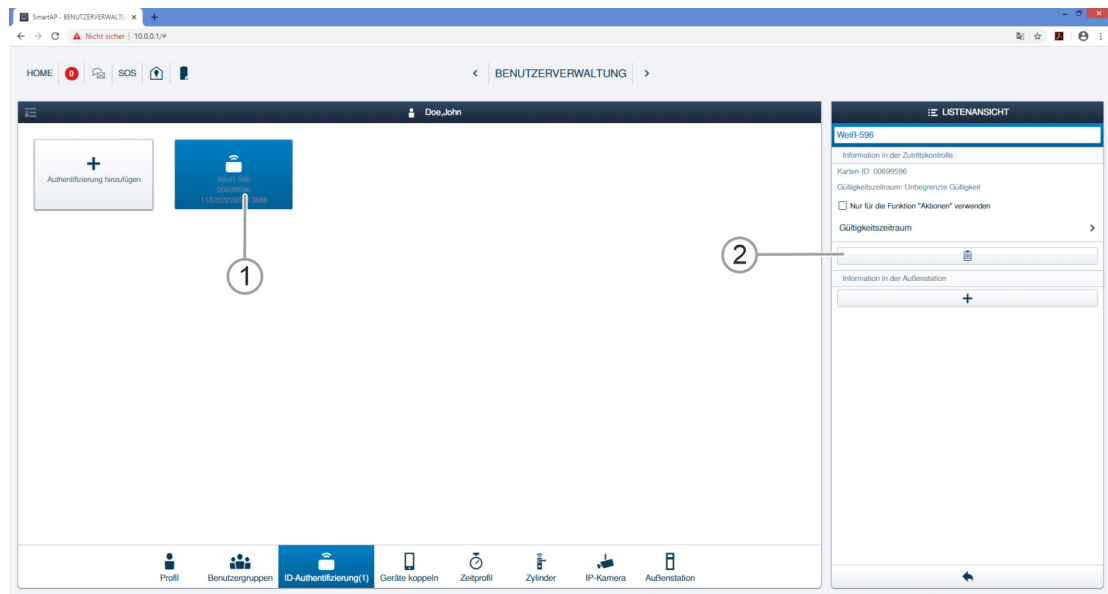


Abb. 134: Authentifizierung löschen

2. Die gewünschte Authentifizierung [1] anklicken.
3. Schaltfläche „Löschen“ [2] klicken.

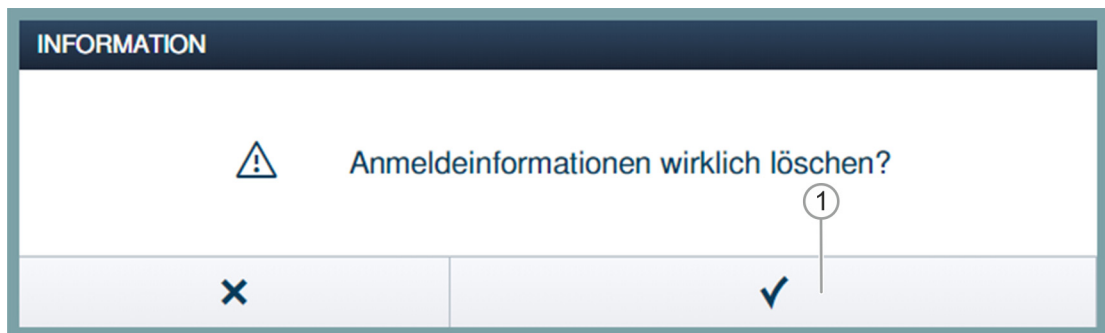


Abb. 135: Bestätigung Authentifizierung löschen

4. Frage mit Schaltfläche [1] bestätigen.
 - Die Authentifizierung ist gelöscht.

5.6.3 Benutzer löschen

Führen Sie zum Löschen eines Benutzers die folgenden Schritte durch:

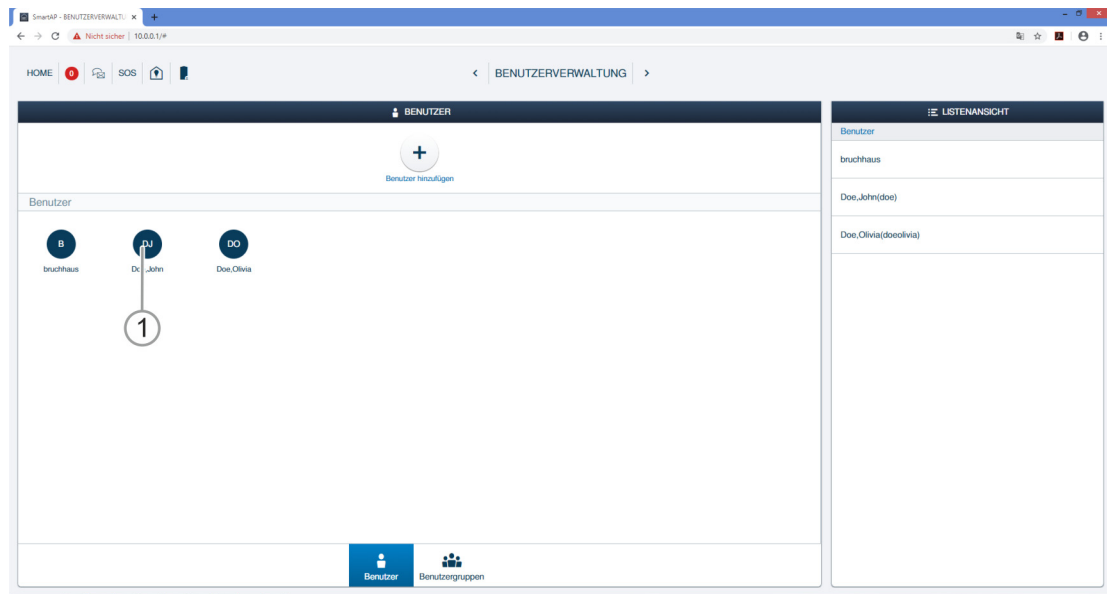


Abb. 136: Benutzer markieren

1. Auf Benutzernamen [1] klicken.

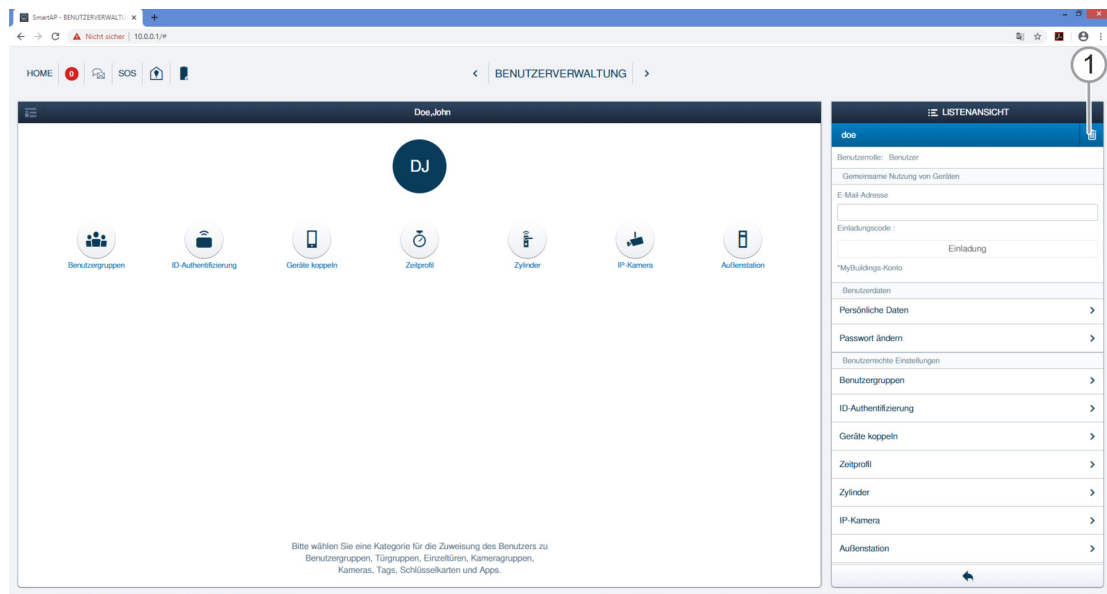


Abb. 137: Benutzer löschen

2. Schaltfläche „Löschen“ [1] klicken.

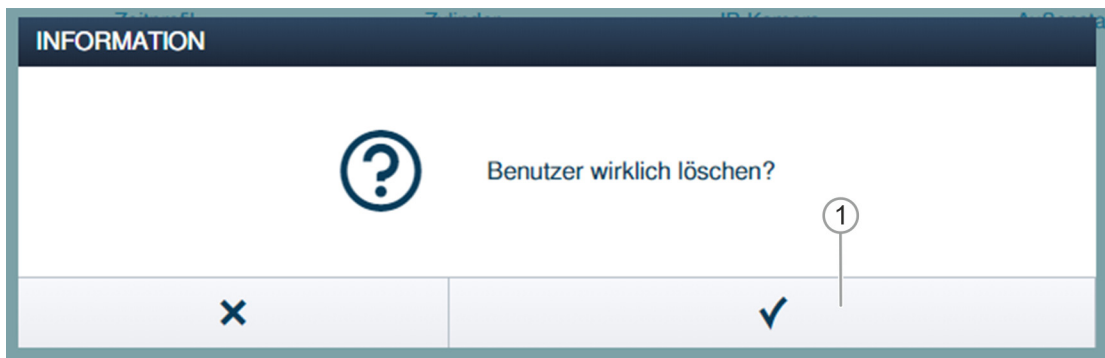


Abb. 138: Bestätigung Benutzer löschen

3. Frage mit Schaltfläche [1] bestätigen.
 - Der Benutzer ist gelöscht.

5.7 Daten aus dem Menü "Zutrittskontrolle" löschen

Das Entkoppeln der Geräte und das Entfernen der Geräte aus den einzelnen Räumen und Etagen erfolgt über den Menüpunkt „Zutrittskontrolle“ im Hauptmenü des „Smart Access Point Pro“.



Abb. 139: Menü "Zutrittskontrolle"

5.7.1 Elektronischer Schließzylinder von Smart Access Point Pro entkoppeln

Führen Sie zum Entkoppeln des „Elektronischer Schließzylinder“ vom „Smart Access Point Pro“ die folgenden Schritte durch:

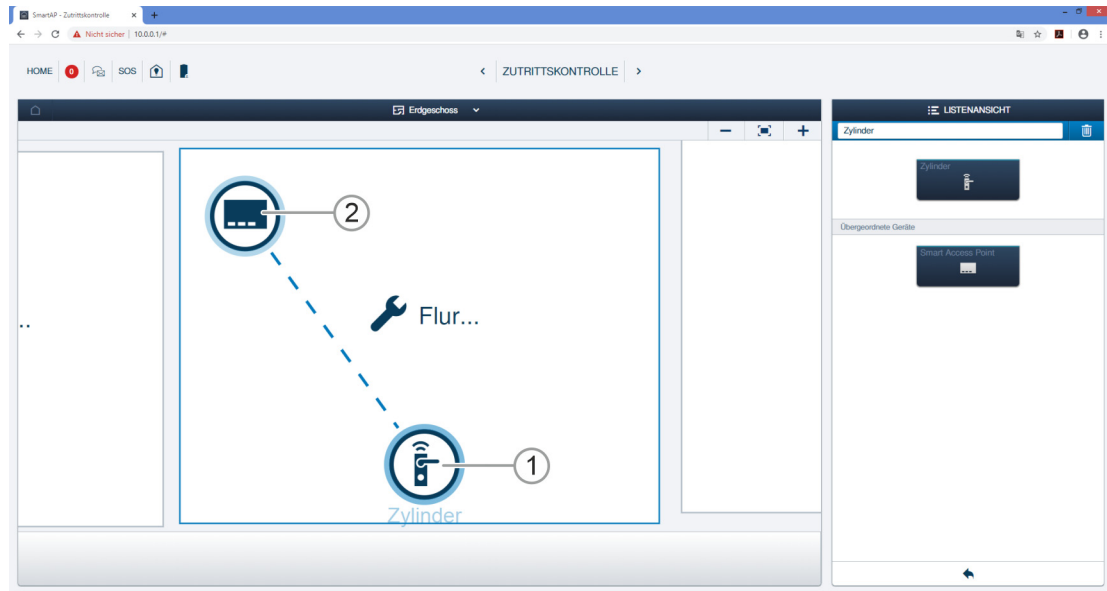


Abb. 140: Kopplung markieren

4. Elektronischer Schließzylinder [1] in der Gebäudestruktur suchen und markieren.
5. Smart Access Point Pro [2] markieren.

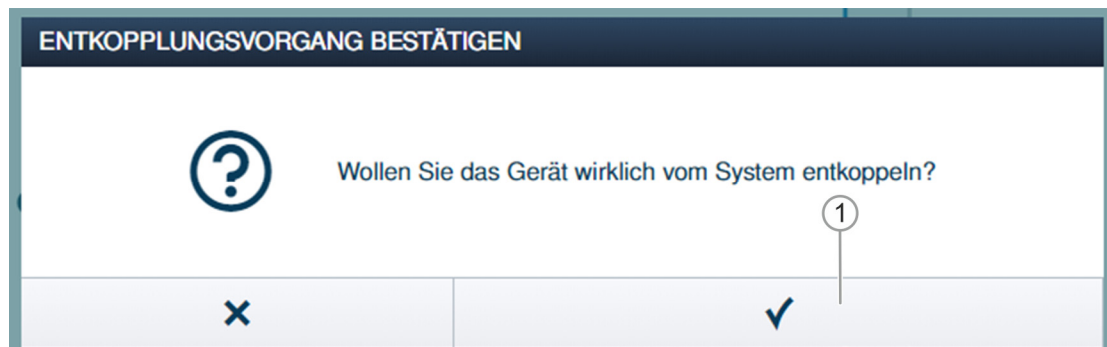


Abb. 141: Bestätigung Entkopplungsvorgang

6. Frage mit Schaltfläche [1] bestätigen.



Abb. 142: Entkopplungsvorgang 1

7. Den Anweisungen folgen und mit Schaltfläche [1] bestätigen.

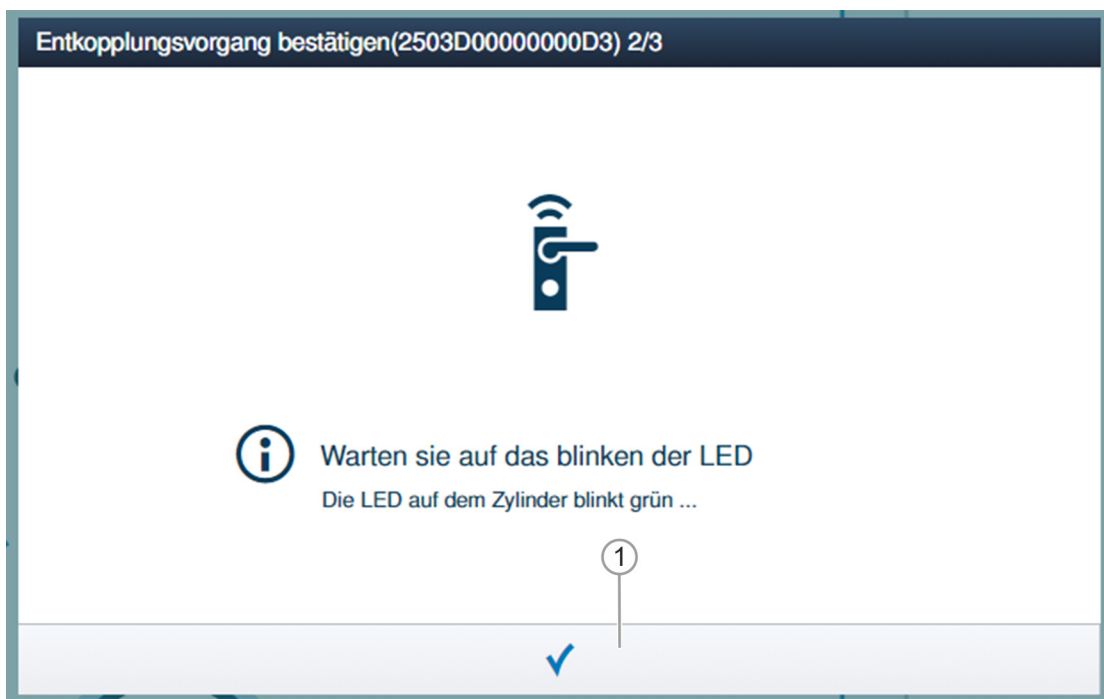


Abb. 143: Entkopplungsvorgang 2

8. Den Anweisungen folgen und mit Schaltfläche [1] bestätigen.

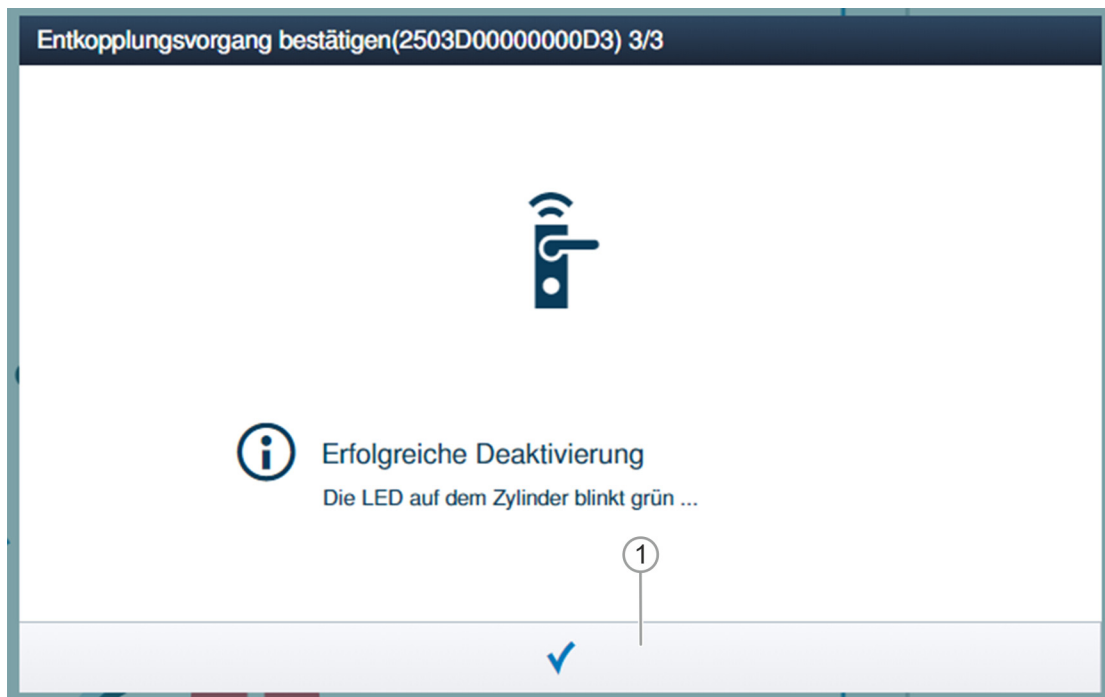


Abb. 144: Entkopplungsvorgang 3

9. Den Anweisungen folgen und mit Schaltfläche [1] bestätigen.

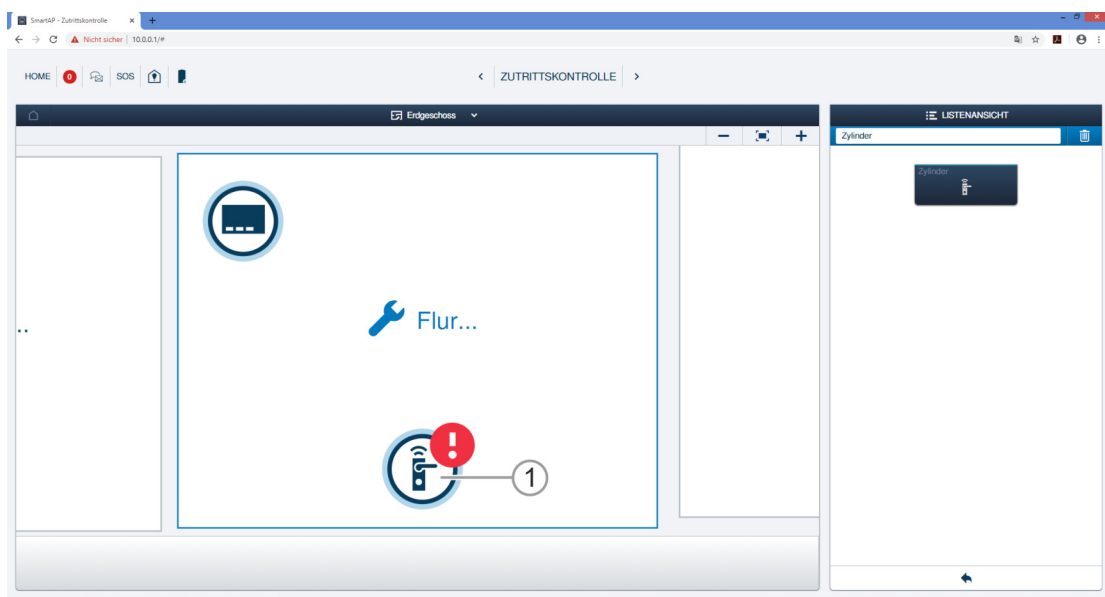


Abb. 145: Zylinder entkoppelt

Die Kopplung zwischen „Elektronischer Schließzylinder“ und „Smart Access Point Pro“ ist aufgehoben. Das Symbol "!" am „Elektronischer Schließzylinder“ [1] zeigt, dass die beiden Geräte nicht mit einander verbunden sind.

5.7.2 Elektronischer Schließzylinder aus dem Raum entfernen

Führen Sie zum Entfernen des „Elektronischer Schließzylinder“ die folgenden Schritte durch:

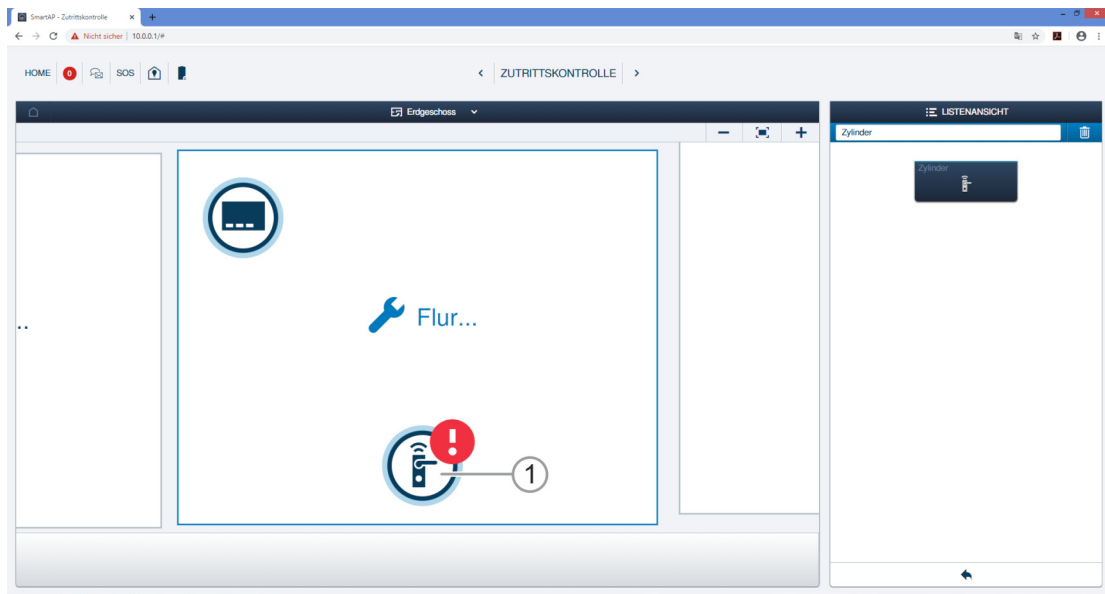


Abb. 146: „Elektronischer Schließzylinder“ aus Gebäudestruktur entfernen

1. Elektronischer Schließzylinder [1] in der Gebäudestruktur suchen und markieren.
2. Schaltfläche „Löschen“ [2] klicken.
 - Der Elektronischer Schließzylinder wird aus dem Raum entfernt.

5.7.3 Smart Access Point Pro aus dem Raum entfernen

Führen Sie zum Entfernen eines „Smart Access Point Pro“ die folgenden Schritte durch:

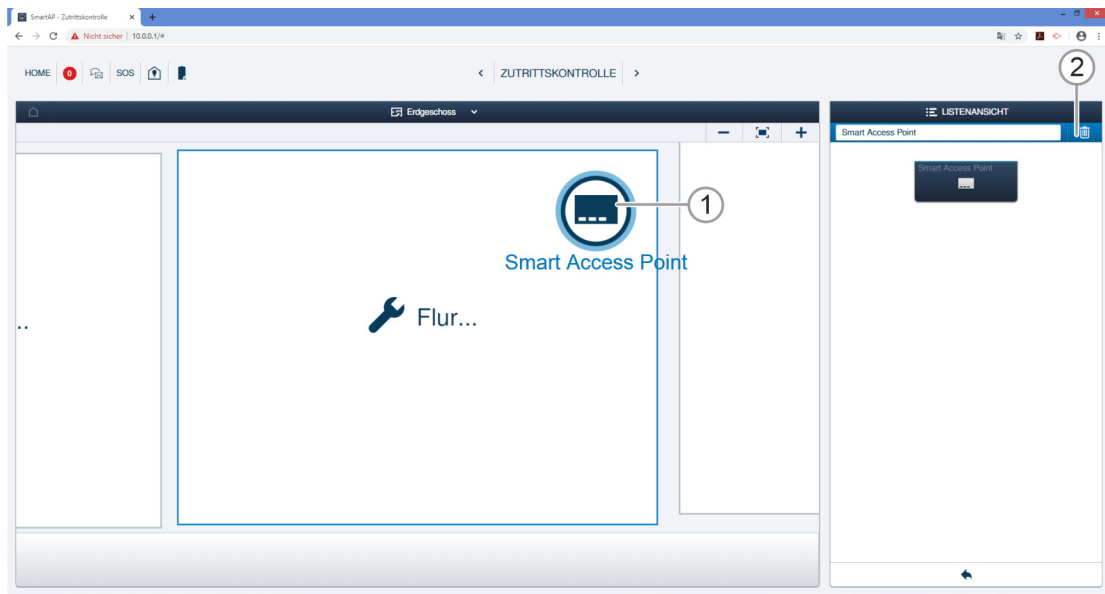


Abb. 147: Smart Access Point markieren

1. „Smart Access Point Pro“ [1] in der Gebäudestruktur suchen und markieren.
2. Schaltfläche „Löschen“ [2] klicken.
 - Der „Smart Access Point Pro“ ist aus dem Raum gelöscht.

5.7.4 Repeater entkoppeln

Führen Sie zum Entkoppeln des Repeaters vom „Smart Access Point Pro“ die folgenden Schritte durch:

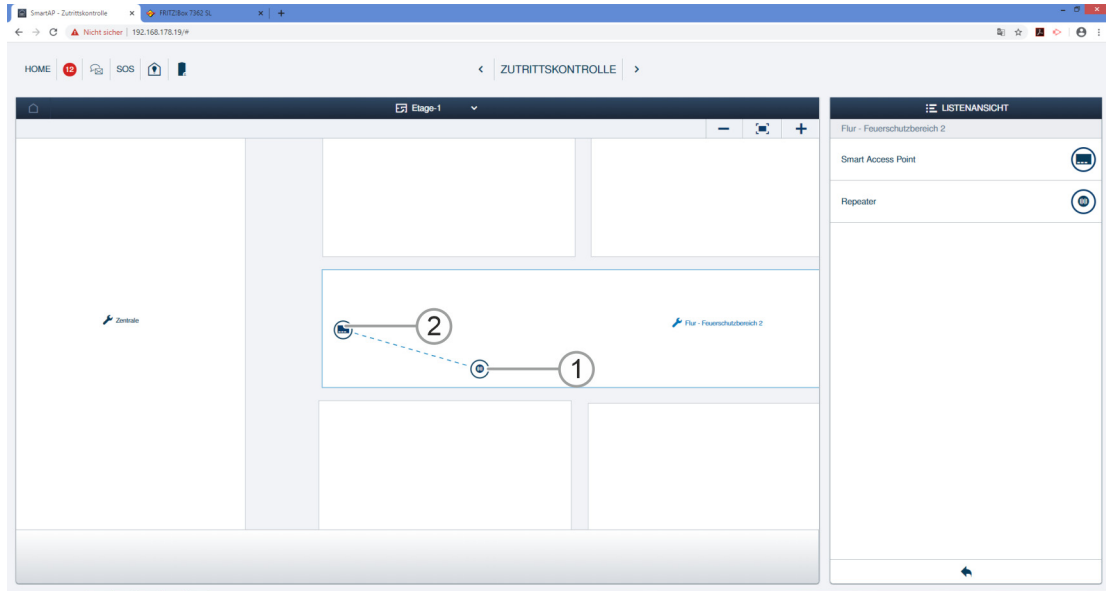


Abb. 148: Kopplung markieren

3. Repeater [1] in der Gebäudestruktur suchen und markieren.
4. Smart Access Point Pro [2] markieren.

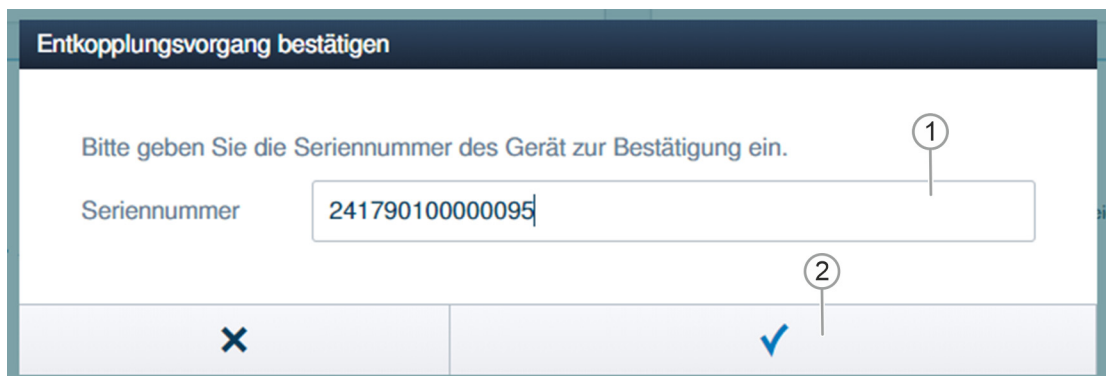


Abb. 149: Bestätigung Entkopplungsvorgang

5. Entkopplungsvorgang mit Eingabe der Repeater-Seriennummer [1] bestätigen.
6. Schaltfläche [2] klicken.

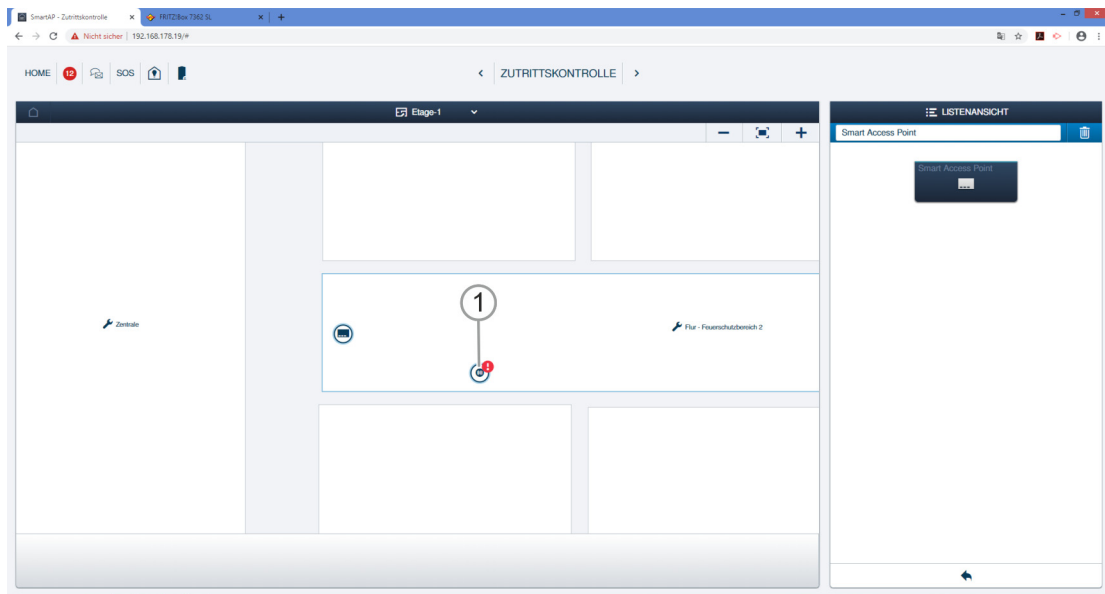


Abb. 150: Repeater entkoppelt

Die Kopplung zwischen Repeater [1] und „Smart Access Point Pro“ ist aufgehoben. Das Symbol "!" am Repeater [1] zeigt, dass die beiden Geräte nicht mit einander verbunden sind.

5.7.5 Repeater aus dem Raum entfernen

Führen Sie zum Entfernen eines Repeaters die folgenden Schritte durch:

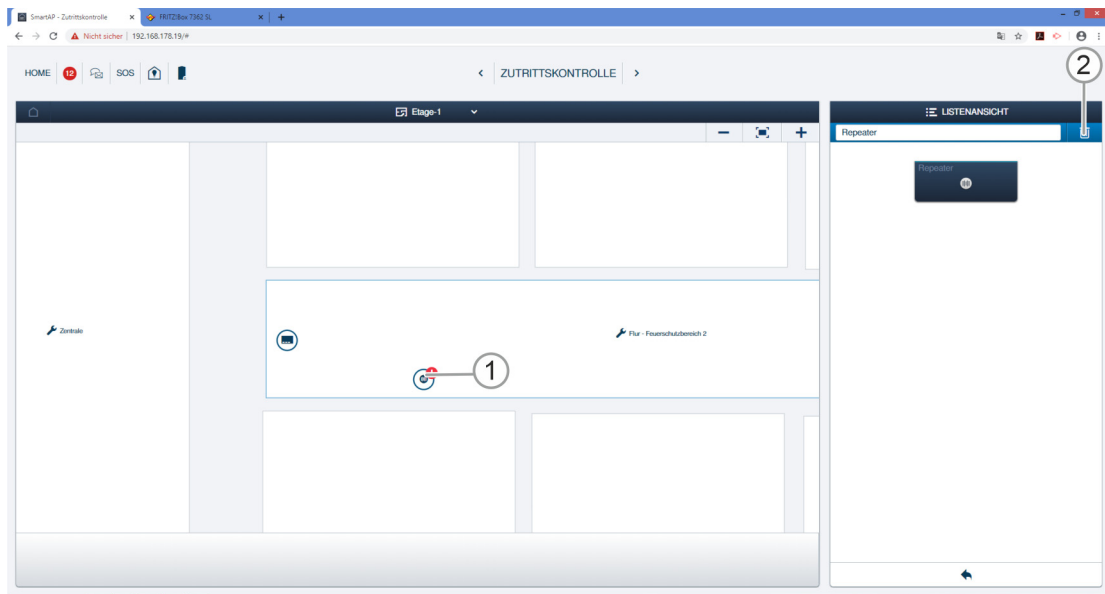


Abb. 151: Repeater markieren

1. Repeater [1] in der Gebäudestruktur suchen und markieren.
2. Schaltfläche „Löschen“ [2] klicken.
 - Der Repeater ist aus dem Raum gelöscht.

5.8 Daten aus dem Menü "Gerätekonfiguration" löschen

Das Löschen von Geräten aus dem System erfolgt über den Menüpunkt „Gerätekonfiguration“ [1] im Hauptmenü des „Smart Access Point Pro“.

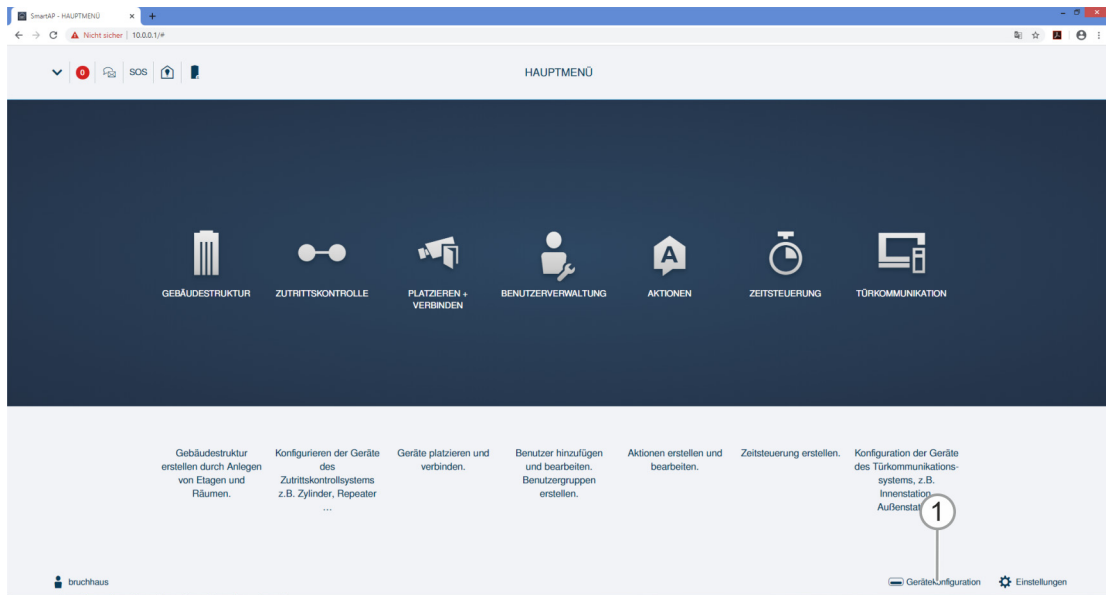


Abb. 152: Menü "Gerätekonfiguration"

5.8.1 Elektronischer Schließzylinder aus dem System löschen

Führen Sie zum Löschen des „Elektronischer Schließzylinder“ die folgenden Schritte durch:

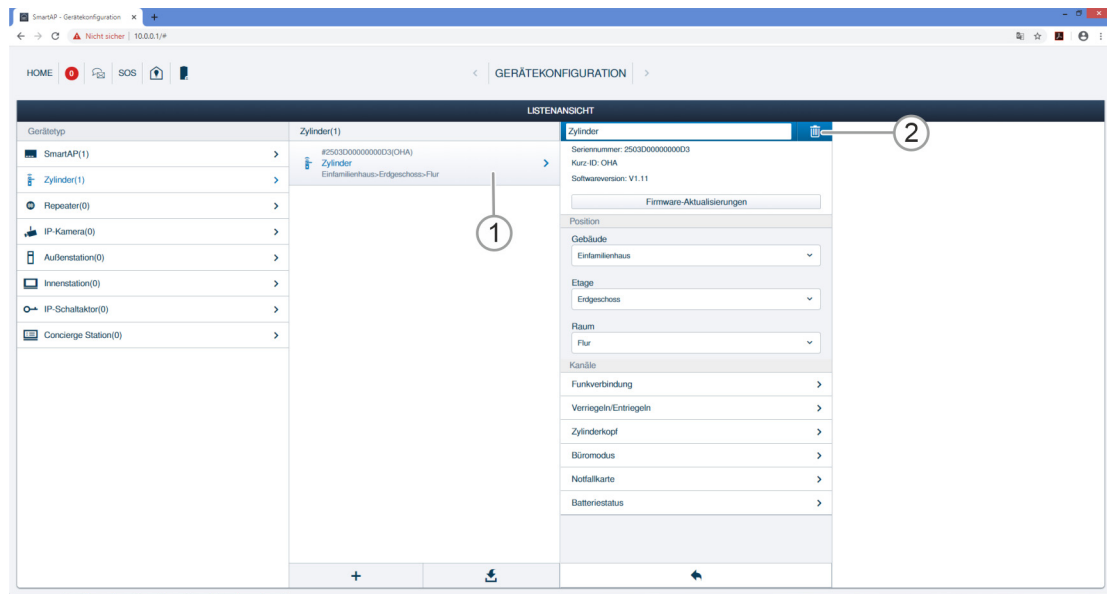


Abb. 153: „Elektronischer Schließzylinder“ löschen

1. Elektronischer Schließzylinder [1] markieren.
2. Schaltfläche „Löschen“ [2] klicken.

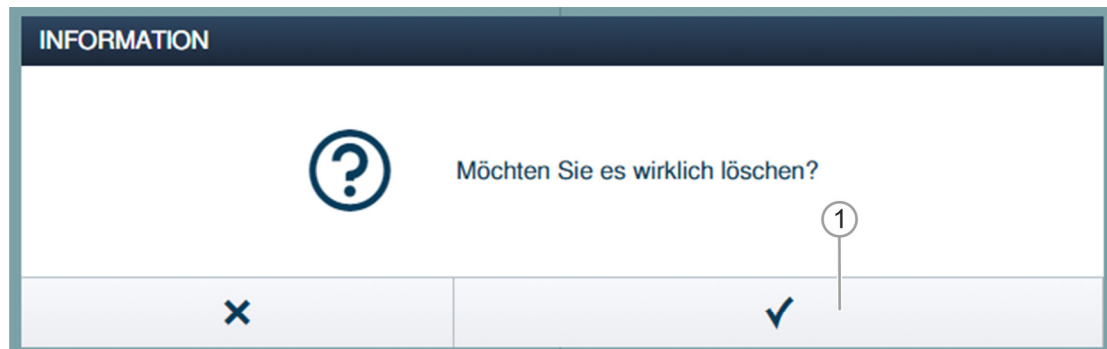


Abb. 154: Bestätigung „Elektronischer Schließzylinder“ löschen

3. Frage mit Schaltfläche [1] bestätigen.
 - Der „Elektronischer Schließzylinder“ ist gelöscht.

5.8.2 Smart Access Point Pro aus dem System löschen

Führen Sie zum Löschen eines „Smart Access Point Pro“ die folgenden Schritte durch:



Abb. 155: „Smart Access Point Pro“ aus System löschen

1. „Smart Access Point Pro“ [1] markieren.
2. Schaltfläche „Löschen“ [2] klicken.



Abb. 156: Bestätigung „Smart Access Point Pro“ löschen

3. Frage mit Schaltfläche [1] bestätigen.
 - Der „Smart Access Point Pro“ ist gelöscht.

5.8.3 Repeater aus dem System löschen

Führen Sie zum Löschen eines Repeaters die folgenden Schritte durch:

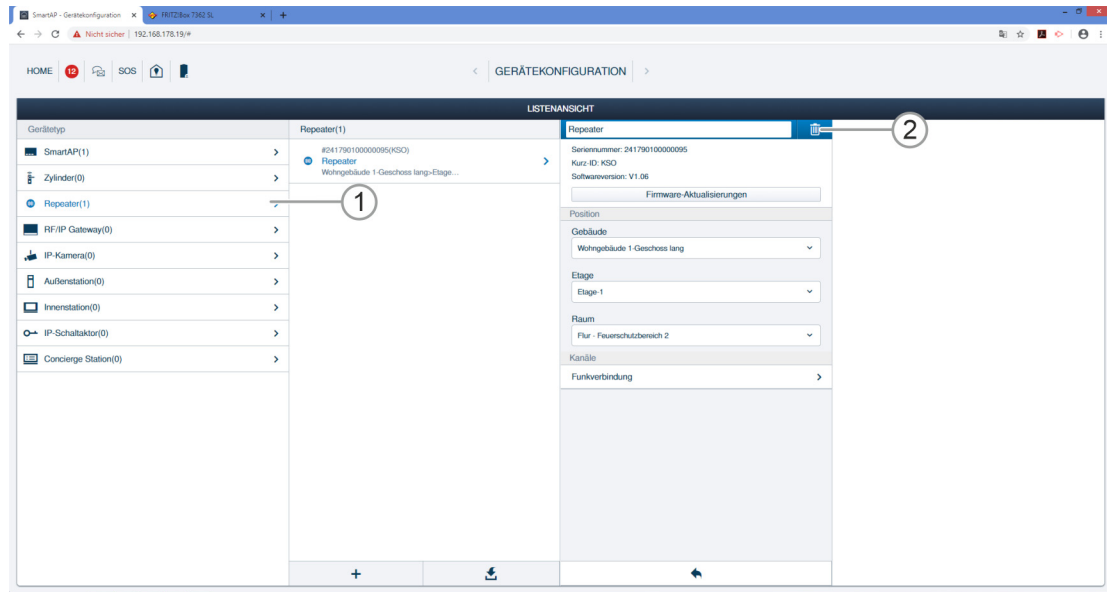


Abb. 157: Repeater aus System löschen

1. Repeater [1] markieren.
2. Schaltfläche „Löschen“ [2] klicken.

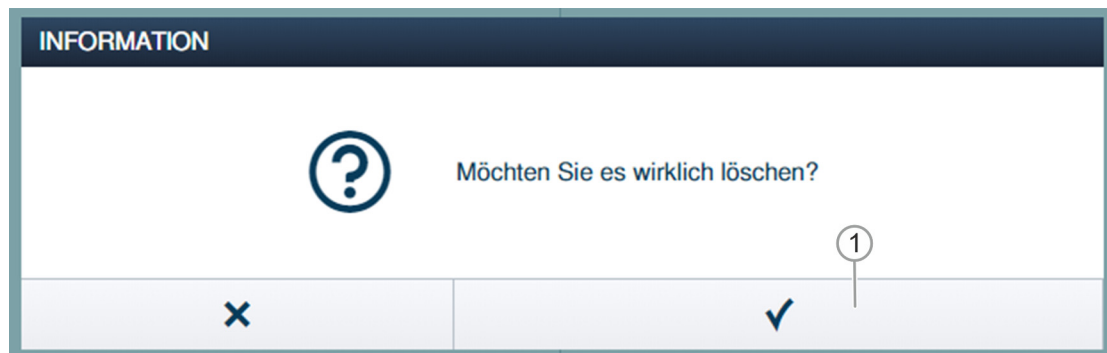


Abb. 158: Bestätigung Repeater löschen

3. Frage mit Schaltfläche [1] bestätigen.
 - Der Repeater ist gelöscht.

5.9 Daten aus dem Menü "Gebäudestruktur" löschen

Das Löschen von Gebäuden, Etagen und Räumen erfolgt über den Menüpunkt „Gebäudestruktur“ [1] im Hauptmenü des „Smart Access Point Pro“.

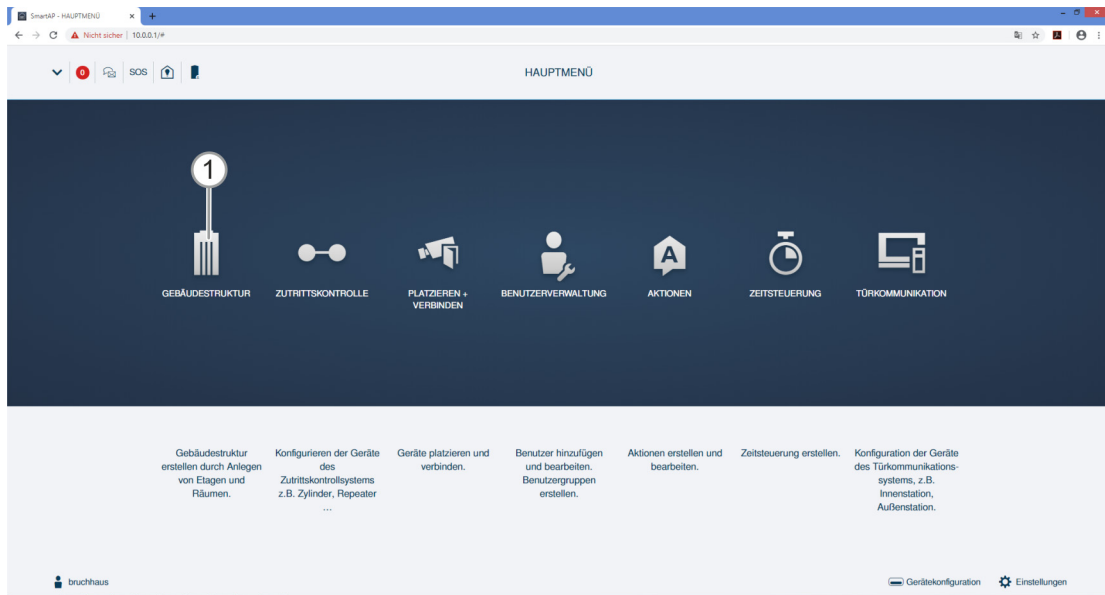


Abb. 159: Menü "Gebäudestruktur"

5.9.1 Räume löschen

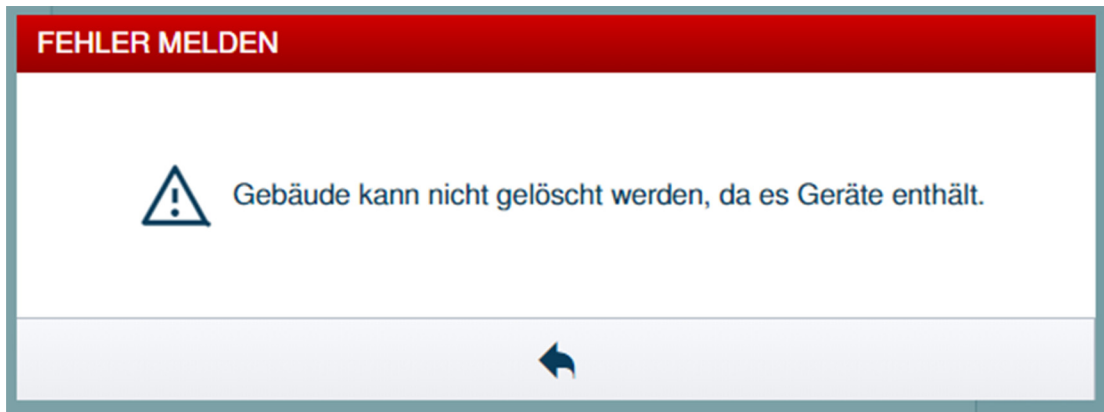


Abb. 160: Warnmeldung



Hinweis

Ein Raum kann nur gelöscht werden, wenn er keine Geräte enthält.

- Alle Geräte des Raums entfernen, bevor der Raum gelöscht wird, siehe Kapitel 5.8 „Daten aus dem Menü "Gerätekonfiguration" löschen“ auf Seite 143

Führen Sie zum Löschen von Räumen die folgenden Schritte durch:

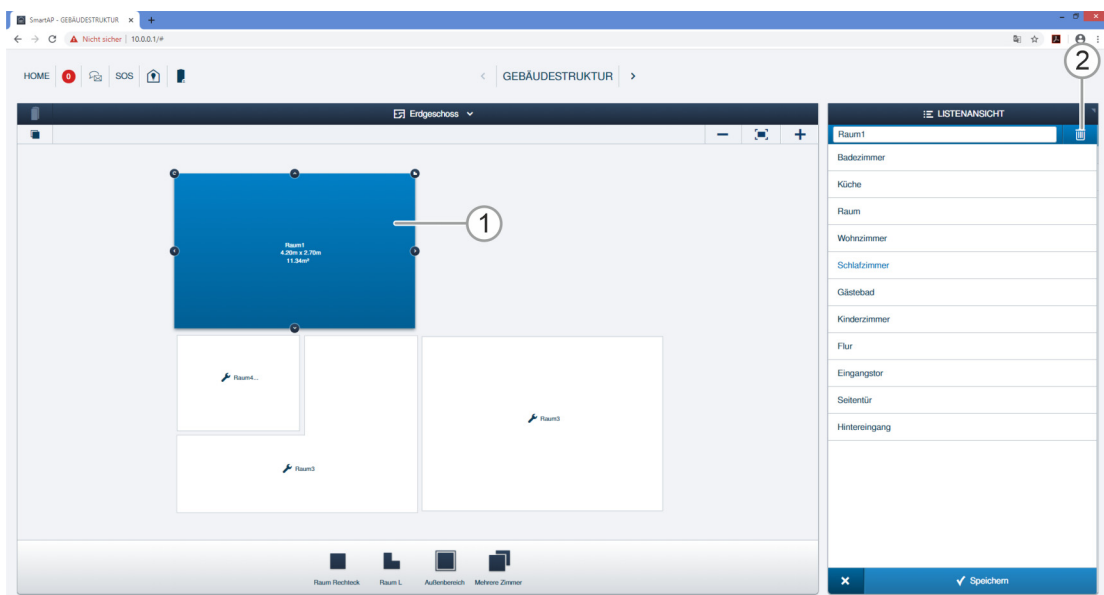


Abb. 161: Raum löschen

1. Raum [1] in der Gebäudestruktur suchen und markieren.
2. Schaltfläche „Löschen“ [2] klicken.
 - Der Raum ist gelöscht.
3. Schritt wiederholen, bis alle gewünschten Räume gelöscht sind.

5.9.2 Etagen löschen



Hinweis

- Eine Etage kann nur gelöscht werden, wenn sie keine Räume enthält.
- Alle Räume der Etage löschen, bevor die Etage gelöscht wird, siehe Kapitel 5.9.1 „Räume löschen“ auf Seite 148

Führen Sie zum Löschen von Etagen die folgenden Schritte durch:

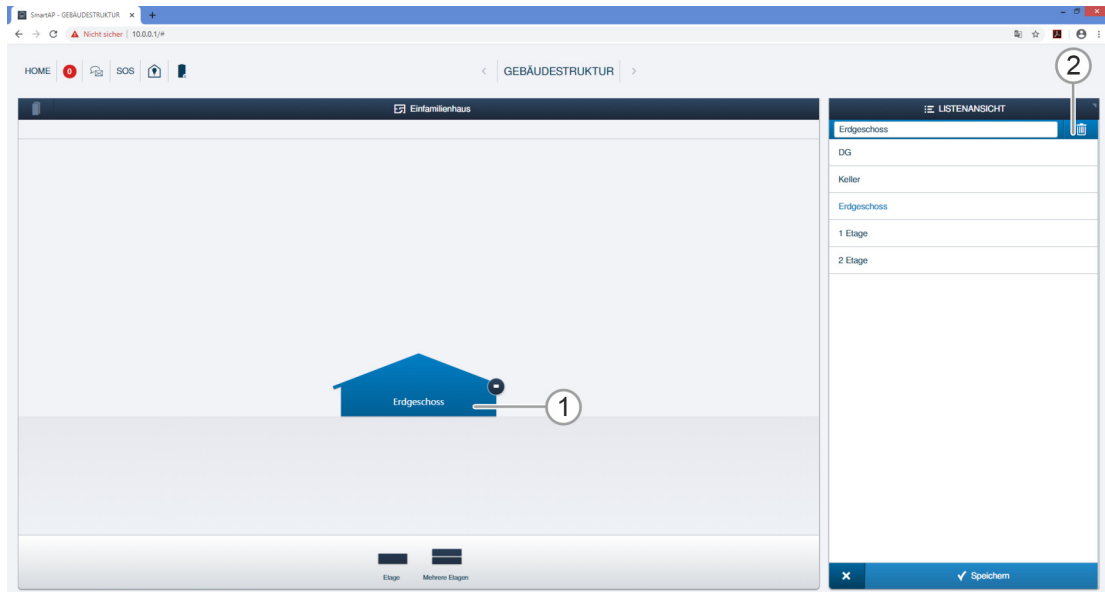


Abb. 162: Etage löschen

1. Etage [1] in der Gebäudestruktur suchen und markieren.
2. Schaltfläche „Löschen“ [2] klicken.
 - Die Etage ist gelöscht.
3. Schritt wiederholen, bis alle gewünschten Etagen gelöscht sind.

5.9.3 Gebäude löschen



Hinweis

Ein Gebäude kann nur gelöscht werden, wenn es keine Etagen enthält.

- Alle Etagen des Gebäudes löschen, bevor das Gebäude gelöscht wird, siehe Kapitel 5.9.2 „Etagen löschen“ auf Seite 149

Führen Sie zum Löschen von Gebäuden die folgenden Schritte durch:

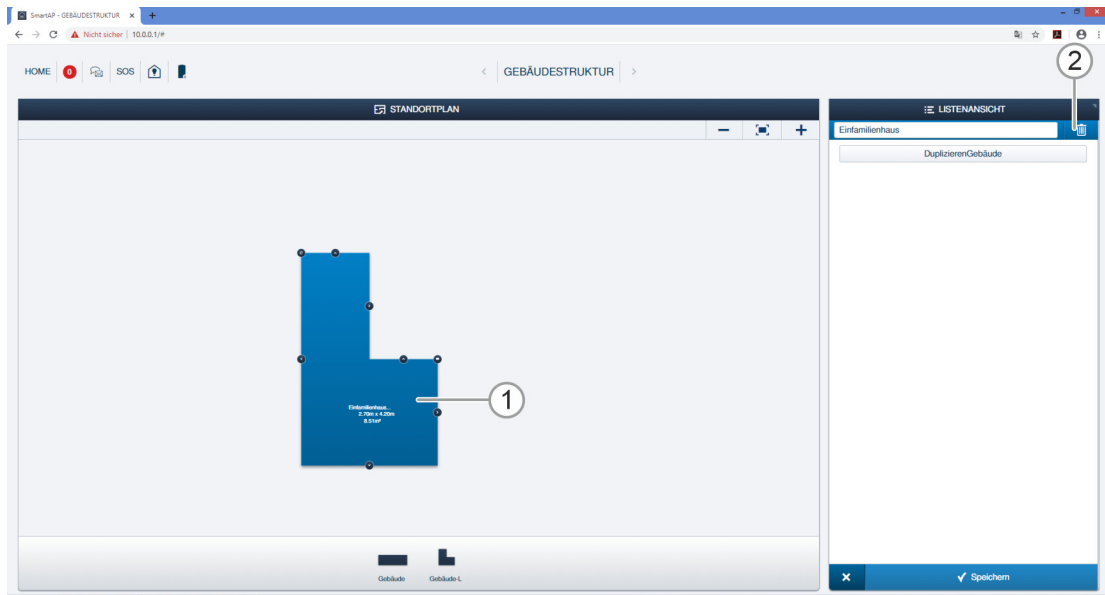


Abb. 163: Gebäude löschen

1. Gebäude [1] in der Gebäudestruktur suchen und markieren.
2. Schaltfläche „Löschen“ [2] klicken.
 - Das Gebäude ist gelöscht.
3. Schritt wiederholen, bis alle gewünschten Gebäude gelöscht sind.

6 Notizen

7 Index

„	
„Elektronischer Schließzylinder“ vorab hinzufügen	29, 46, 50, 51
A	
Anwendungsbeispiele	5, 66
Anwendungsbereiche	15
Arbeitsweisen	57
Authentifizierung löschen	138
B	
Backup	54
Benutzer anlegen	125, 126
Benutzer löschen	140
Benutzergruppen anlegen	127
Benutzerverwaltung	29, 45, 49, 52, 92, 121, 125
Busch-AccessControl	6
Busch-AccessControl und smartIP	8
D	
Daten aus dem Menü	135, 142, 151, 155, 156
Designlinien	13
E	
Einführung in Busch-AccessControl	6
Einsatz	14
Elektrofachkraft	6
Elektronischer Schließzylinder	29, 45, 48, 53, 95, 116
Elektronischer Schließzylinder aus dem Raum entfernen	53, 146
Elektronischer Schließzylinder aus dem System löschen	53, 152
Elektronischer Schließzylinder mit Smart Access Point koppeln	29, 49, 90, 119
Elektronischer Schließzylinder von Smart Access Point Pro entkoppeln	53, 143
Etagen	157, 158
Etagen anlegen	105
F	
Funktionsprinzipien	57
G	
Gebäude	158
Gebäude anlegen	102
Gebäudestruktur	29, 48, 51, 52, 67, 69, 71, 74, 79, 83, 89, 92, 95, 98, 99, 101
Geräte hinzufügen	45
Geräte löschen	53
Gerätekonfiguration	49, 52, 92
Geräteübersicht	17
Grundlagen	13
Grundlagen strukturierter Verkabelung	9, 64, 87
H	
Handbuch	5
Hinweise zum Handbuch	5
I	
Inbetriebnahme	29
Inbetriebnahme	31
Inbetriebnahme	55
Inbetriebnahme Übersicht	29
IP-Adresse an einem PC angleichen	43
K	
Kapazität	61, 66, 68, 70, 72, 76, 80, 84
M	
Montagemöglichkeiten	22
N	
Notizen	159
P	
PC mit	31, 54, 55
Planungs- / Anwendungsinformationen	13, 57
Projekt sichern (Backup)	54
Projekt wiederherstellen (Restore)	54
Q	
Qualifikation des Personals	6
R	
Räume	156, 157
Räume anlegen	107
Reichweite	61, 66, 68, 70, 72, 76, 80, 84
Repeater	29, 51, 52, 53, 122, 123, 148, 150, 154
RESET (System / Geräte zurücksetzen)	55
Restore	54
S	
Schließrecht löschen	136
Schließzylinder	18
Smart	147, 153
smartIP	8
Störquellen	90
Strukturierte Verkabelung	9, 64, 87
Systemgeräte	19
Systemmodi Auswahl	31, 34, 37
U	
Übersicht	5, 31
Übersicht Inbetriebnahme	29
V	
Verwaltungssoftware im	91
Voraussetzungen	22, 29
Z	
Zielgruppe	6
Zubehör	21
Zurücksetzen Geräte	55

Zurücksetzen System).....55

Zutrittskontrolle49, 52, 92, 109

Busch-Jaeger Elektro GmbH
Ein Unternehmen der ABB-Gruppe

Postfach
58505 Lüdenscheid

Freisenbergstraße 2
58513 Lüdenscheid

<https://BUSCH-JAEGER.de>
info.bje@de.abb.com

Zentraler Vertriebsservice:
Tel.: +49 2351 956-1600
Fax: +49 2351 956-1700